SMT IPMI

User's Guide

Revision 2.0

The information in this User's Manual has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL SUPER MICRO COMPUTER, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: Refer to Supermicro's web site for FCC Compliance Information.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".

WARNING: Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

Manual Revision 1.0b

Release Date: September 15, 2010

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2010 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About this User's Guide

This user guide is written for system integrators, PC technicians and knowledgeable PC users who intend to configure the IPMI settings supported by the Nuvoton WPCM450 BMC Controller embedded in Supermicro's motherboards. It provides detailed information on how to configure the IPMI settings provided by the WPCM450 Controller.

Note: Nuvoton Technology is a subsidiary of Winbond Corp.

User's Guide Organization

Chapter 1 provides an overview on the Nuvoton WPCM450 Controller. It also introduces IPMI, its features and its configuration settings.

Chapter 2 provides detailed instructions on how to configure the IPMI settings supported by the WPCM450 Controller.

Chapter 3 provides the answers to frequently asked questions.

Conventions Used in This User's Guide

Pay special attention to the following symbols for proper installation and to prevent damage to the system or injury to yourself.

Warning: Important information given to prevent erroneous RAID configuration and to ensure proper system setup,

Note: Additional information given to ensure correct RAID configuration setup.

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)

Asia-Pacific

Address:	Super Micro Computer, Inc. 4F, No. 232-1, Liancheng Rd. Chung-Ho 235, Taipei County Taiwan, R.O.C.
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3991
Web Site:	www.supermicro.com.tw
Technical Support:	
Email:	support@supermicro.com.tw
Tel:	886-2-8228-1366, ext.132 or 139

Notes

Table of Contents

Preface

Chapter 1 Introduction

1-1 Overview of the Nuvoton WPCM 450 BMC Controller 1-1
WPCM450 DDR2 Memory Interface 1-1
WPCM450 PCI System Interface 1-1
Supermicro IPMI Features 1-2
1-2 WPCM450 Block Diagram 1-3
1-3 Introduction to the IPMI Platform 1-3
1-4 Motherboards Supported 1-4
1-5 An Important Note to the User 1-4

Chapter 2 Configuring the IPMI Settings

2-1 Configuring the IP/MAC Addresses for Remote Servers 2-1
Using the IPMICFG Utility to Set the IP/MAC Addresses for Remote Servers 2-1
Using the BIOS Utility to Set the IP/MAC Addresses for Remote Servers 2-2
2-2 Connecting to the Remote Server 2-3
Using the IPMIView to Connect to the Remote Server 2-3
Using the Browser to Connect to the Remote Server 2-3
2-3 Accessing the Remote Server via Console Redirection Using the Browser 2-4
To Log In to the Remote Console 2-4
2.4 IPMI Main Screen 2-5
2.5 System Status 2-6
2.6 Server Health 2-7
2.6.1 Sensor Readings 2-8
2.6.2 Event Log 2-10
2.7 Configuration 2-11
2.7.1 Configuring the Alerts Settings 2-12
2.7.2 Configuring Date and Time Settings 2-14
2.7.3 Configuring the Light-Weight Directory Access Protocol (LDAP) Settings 2-15
2.7.4 Active Directory Settings 2-16
2.7.5 Configuring the Radius Settings 2-18
2.7.6 Configuring the Mouse Mode Settings 2-19
2.7.7 Configuring Network Settings 2-20
2.7.8 Configuring Dynamic DNS (Domain Name System) Settings 2-22
2.7.9 Configuring the Remote Session Settings 2-23

2.7.10 Configuring the SMTP Settings 2-24
2.7.11 Configuring the SSL (Secure Sockets Layer) Certification 2-25
2.7.12 Configuring Users Settings 2-26
2.8 Remote Control 2-28
2.8.1 Launching Console Redirection 2-29
2.8.2 Remote Control - Server Power Control 2-50
2.8.3 Remote Control-Launch SOL 2-51
2.9 Virtual Media 2-53
2.9.1 Configuring USB Floppy & Flash Device Settings 2-54
2.9.2 Configuring CD ROM Image File Settings 2-55
2.10 Maintenance 2-57
2.10.1 Maintenance - Firmware Update 2-58
2.10.2 Maintenance - Unit Reset 2-60
2.10.3 Maintenance - IKVM Reset 2-61
2.10.4 Maintenance - Factory Default 2-62
2.10.5 Maintenance - IPMI Configuration 2-63
2.11 Miscellaneous 2-64
2.11.1 Miscellaneous - POST Snooping 2-64
2.11.2 Miscellaneous - UID Control 2-65

Chapter 3 Frequently Asked Questions

3-1 Frequently Asked Questions 3-1

Appendix A Flash Tools

A-1 Overview A-1
A-2 Reference A-1
A-3 Using Aten Flash Tools in the DOS Environment A-1
Firmware Updating via KCS Channels A-2
Dumping Firmware from the BMC via KCS channels A-3
A-4 Windows/Linux Version of Flash Tools A-4

Appendix B Introduction to SMASH

B-1 Overview B-1
How SMASH works B-1
SMASH Compliance Information B-2
B-2 An Important Note to the User B-2
B-3 Using SMASH B-3
B-4 Initiating the SMASH Protocol B-3
To Initiate SMASH Automatically B-3
B-5 SMASH-CLP Main Screen B-4
B-6 Using SMASH for System Management B-4
B-7 Definitions of Command Verbs B-5

B-8 SMASH Commands B-7
B-9 Standard Command Options B-8
B-10 Target Addressing B-9
Terms Used in the Target Addressing Diagram B-9

Chapter 1

Introduction

1-1 Overview of the Nuvoton WPCM 450 BMC Controller

The Nuvoton WPCM450, a Baseboard Management Controller (BMC), supports PCI-based 2D/VGA Graphics cores, multi-media virtualization, and Keyboard/Video/Mouse Redirection (KVMR) modules. The WPCM450 Controller is ideal for server management platforms.

The WPCM450 interfaces with the host system via PCI connections to communicate with the Graphics core. It supports USB 2.0 and 1.1 for remote KVM emulation. It also provides LPC interface to control Super IO functions. The WPCM450 is connected to the network via an external Ethernet PHY module or shared NCSI connections.

The WPCM450 communicates with onboard components via SMBus interface, PECI (Platform Environment Control Interface) buses, and General Purpose I/O ports.

WPCM450 DDR2 Memory Interface

The WPCM450 Controller supports a 16-bit DDR2 memory module with a speed of up to 220 MHz. The motherboard supports 128 MB of memory which is shared between the BMC and onboard graphics card. For best signal integrity, the WPCM450 provides point-to-point connections.

WPCM450 PCI System Interface

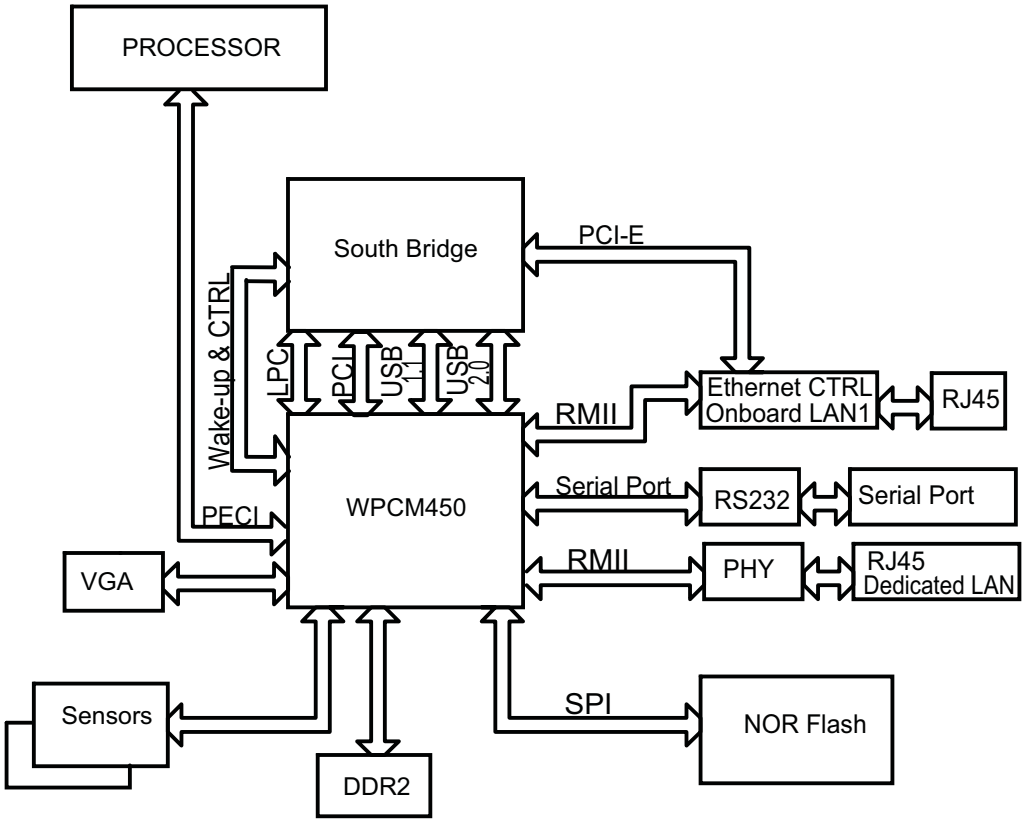
The WPCM450 provides 32-bit, 33 MHz 3.3V PCI interface, compliant with PCI Local Bus Specification Rev. 2.3. The PCI system interface connects to the onboard PCI Bridge and is used by the graphics controller.

Supermicro IPMI Features

1. Remote KVM (graphics) console
2. Virtual Media and ISO images
3. Remote server power control
4. Remote Serial over LAN (text console)
5. Event Log support
6. Automatic Notification and Alerts (SNMP and email)
7. Hardware Monitoring
8. Overall health display on the main page
9. Out of band management through shared or dedicated LAN
10. Option to change LAN connection interface at Runtime
11. VLAN
12. RMCP & RMCP+ protocols supported
13. SMASH/CLP
14. Secure command line interface (SSH) and Telnet
15. WSMAN and WS-CIM
16. RADIUS authentication support
17. Secure browser interface (Secure socket layer - SSL support)
18. Lightweight Directory Access Protocol (LDAP) supported
19. DCMI 1.0 support
20. Backup and restore the configuration file
21. Factory defaults from web support
22. Video quality settings
23. Record video and play
24. Server data/information
25. Preview of the remote screen on the main page
26. Update Firmware through browser and OS
27. OS-independent

1-2 WPCM450 Block Diagram

The following diagram represents a typical system setup for the WPCM450 Controller.



1-3 Introduction to the IPMI Platform

The Intelligent Platform Management Interface (IPMI) provides remote access to multiple users at different locations for networking. It also allows a system administrator to monitor system health and manage computer events remotely.

IPMI operates independently from the operating system. When used with an IPMI Management utility installed on the motherboard, the WPCM450 BMC Controller will connect the South Bridge to other onboard components, providing remote network interface via serial links. With the WPCM450 Controller and the IPMI firmware built in, the Supermicro motherboard allows the user to access, monitor, diagnose, and manage a remote server via Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

1-4 Motherboards Supported

This version of SMT IPMI is supported by the motherboards listed in the table below. If your motherboard is not included in the table, please refer to the motherboard product page on our website @www.supermicro.com and download the right BMC/IPMI user's guide for your motherboard.

Intel Dual-Processor Motherboards supported (-F models only)	Intel Single-Processor Motherboards supported (-F models only)	AMD Motherboards supported (for -F models only)
X8DTL-3F/-6F/iF	X7SPA-HF	H8DGG-QF
X8DTN+-F	X7SPE-HF	H8DGT-HF/HIBQF
X8DTU-6F+/6TF+/LN4F+/TF	X8SI6-F	H8DGU-F
	X8SIA-F	H8SGL-F
	X8SIE-F/LN4F	H8SCM-F
	X8SIL-F/F+	
	X8SIT-F	

1-5 An Important Note to the User

The graphics shown in this user's guide were based on the latest information available at the time of publishing of this guide. The IPMI screens shown on your computer may or may not look exactly like the screen shown in this user's guide.

Chapter 2

Configuring the IPMI Settings

With the Nuvoton WPCM450 BMC Controller and the IPMIView firmware built in, Supermicro motherboards allow the user to access, monitor, manage and interface with multiple systems in various remote locations. The necessary firmware for accessing and configuring the IPMI settings are available on Supermicro's website at hppt://www.supermcro.com/products/nfo/ipmi.cfm. This section provides detailed information on how to configure the IPMI settings.

2-1 Configuring the IP/MAC Addresses for Remote Servers

Note: The DHCP (Dynamic Host Configuration Protocol) is on by default. To change the manufacturer default setting, please use the ipmicfg utility or the BIOS Setup utility.

Using the IPMICFG Utility to Set the IP/MAC Addresses for Remote Servers

1. Run the ipmicfg utility from the bootable CD that came with your shipment.

2. Follow the instructions given in the Readme.txt file to configure Gateway IP/ Netmask IP addresses, enable/disable DHCP, and configure other IPMI settings.

- IPMICFG Version 1.35 (Build 2010-04-28) Copyright 2010 Super Micro Computer, Inc. Usage: IPMICFG Parameters (Example: IPMICFG -m 172.31.1.84)

-m	Shows IP and MAC
-m IP	Sets IP (format: ###.###.###.###)
-a MAC	Sets MAC (format: ##:##:##:##:##:##)
-k	Shows Subnet Mask
-k Mask	Sets Subnet Mask (format: ###.###.###.###)
-dhcp	Gets the DHCP status
-dhcp on	Enables the DHCP
-dhcp off	Disables the DHCP
-g	Shows Gateway IP
-g IP	Sets Gateway IP (format: ###.###.###.###)
-r	BMC cold reset

-garp on	Enables the Gratuitous ARP
-garp off	Disables the Gratuitous ARP
-fd	Resets to the factory defaults
-ver	Gets the firmware revision
-vlan	Gets VLAN status
-vlan on (VLANtag)	Enables the VLAN and sets the VLAN tag (If VLAN tag is not given, it uses previously saved value.)
-vlan off	Disables the VLAN
-raw	Sends a RAW IPMI request and print the response. Format: NetFn LUN Cmd [Data1...DataN].
-sdr	Shows SDR records and reading
-sdr del <SDR ID>	Deletes SDR record
-sdr backup <FILE>	Backups SDR to file
-sdr restore <FILE>	Restores SDR from file
-sdr ver [<V1><v2>]	Retrieves and sets SDR version (V1, V2)
-sel info	Shows SEL info
-sel list	Shows SEL records
-sel del	Deletes all SEL records
-fru info	Shows FRU inventory area info
-fru list	Shows all FRU values
-fru help	Shows FRU Write help
-fru cthelp	Shows chassis type code
-fru <Field>	Shows FRU field value
-fru <Field> <Value>	Writes FRU
-fru backup <File>	Backs up FRU to file
-fru restore <File>	Restores FRU from file
-fru ver [<V1> <V2>]	Retrieves and sets FRU version (V1, V2)

Using the BIOS Utility to Set the IP/MAC Addresses for Remote Servers

1. Go to the BIOS by pressing the <Del> key at bootup.

2. Select *IPMI* from the Advanced Menu.

3. Select *LAN Configuration* from the IPMI submenu.

4. Click <IP Address Source>. Select *Static* and press <Enter>. The onboard BIOS will automatically set the IP Address, MAC Address, Gateway, and Subnet Mask.

5. Once IP Address, MAC Address, Gateway, and Subnet Mask are set, click <Update LAN Settings>. Select *Yes* and press <Enter> to update IPMI LAN settings.

6. Go to the Exit menu. Select *Save Changes & Exit* and press <Enter> to save changes and exit the BIOS.

2-2 Connecting to the Remote Server

Using the IPMIView to Connect to the Remote Server

1. Connect a LAN cable to the onboard LAN1 port or the dedicated IPMI LAN port.

2. Choose a computer that is connected to the same network and open the IPMIView utility.

3. Go to File>New>System. Enter the System Name, IP Address of LAN1 (or the dedicated LAN, and the Description in the appropriate fields, and press <Enter>.

4. Select the system from the IPMI Domain. Enter the Login ID and Password in the appropriate fields to log in to the IPMIView utility.

Using the Browser to Connect to the Remote Server

1. Connect a LAN cable to the onboard LAN1 port or the dedicated IPMI LAN port.

2. Choose a computer that is connected to the same network and open the browser.

3. Enter the IP address of each server that you want to connect to in the address bar of your browser.

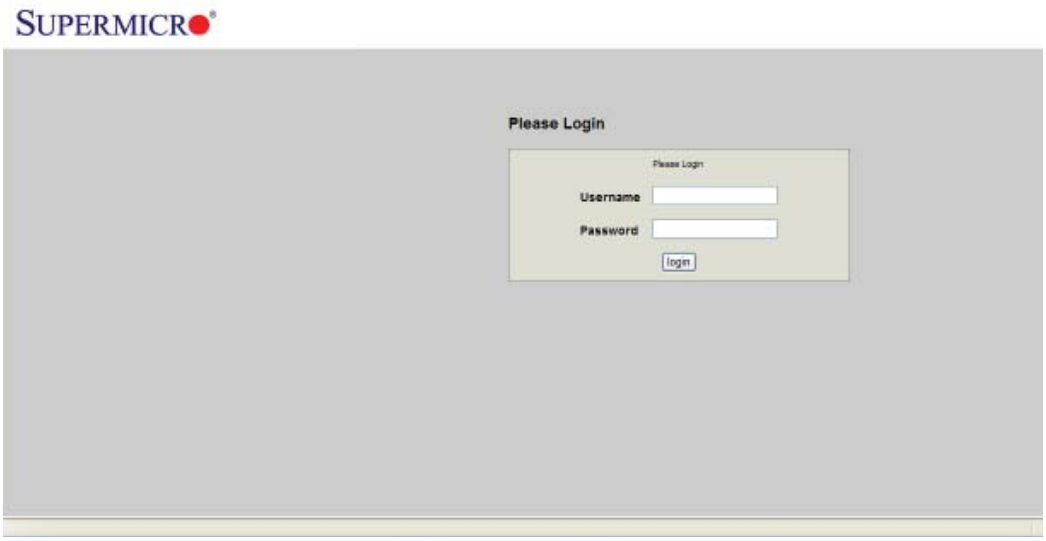
4. Once the connection is made, the Login screen as shown on the next page will display.

Note: The default network setting is "Failover", which will allow the IPMI to connect to the network through a shared LAN port (onboard LAN Port 1 or 0) or through the IPMI_Dedicated_LAN_Port. If the IPMI must be connected through a specific port, please change the LAN configuration setting under the Network Settings.

2-3 Accessing the Remote Server via Console Redirection Using the Browser

To Log In to the Remote Console

Once you are connected to the remote server via IPMI Console Redirection, the following IPMI Login screen will display.



1. Enter your Username in the *Username* fields.

Note: The manufacturer default username and password are ADMIN/ADMIN. Once you have logged into the BMC using the manufacturer default password, be sure to change your password for security purpose.

2. Enter your Password in the *Password* box and click <Login>.

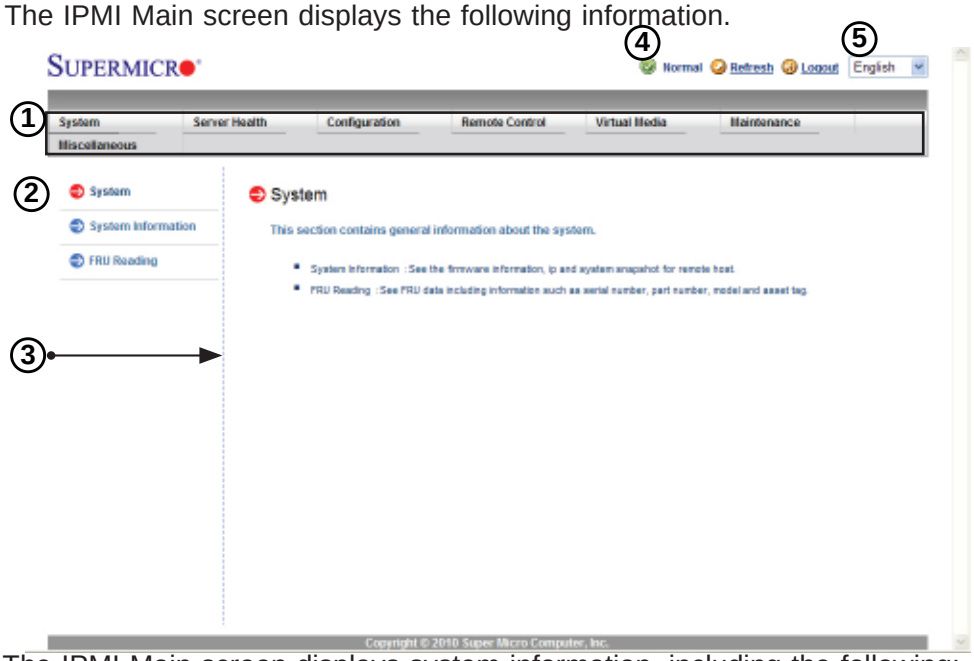
3. The Home Page will display as shown on the next page.

Note 1: To use the IPMIView utility for Console Redirection, please refer to the IPMIView User's Guide for instructions.

Note 2: The *Administrator* account cannot be deleted.

2.4 IPMI Main Screen

The IPMI Main screen displays the following information.



The IPMI Main screen displays system information, including the following:

1. The Menu Bar: The menu bar on the top displays System Information, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, and Miscellaneous. Click an item on the Menu Bar to access an IPMI feature and configure its settings.

2. The Options Window: This window displays IPMI submenu items. Click an item in this window to configure the setting.

3. The Main Display Area: This area displays the contents of the particular section. Click an item in this area to configure the setting.

4. System Health Status: This icon displays the health status of the server.

- Green: It indicates that the server is normal.

- Orange: At least an alert has occurred. Take proper actions to ensure system health.

- Red: At least one critical condition has occurred. Immediate attention is required to resolve the critical condition for the server to function normally.

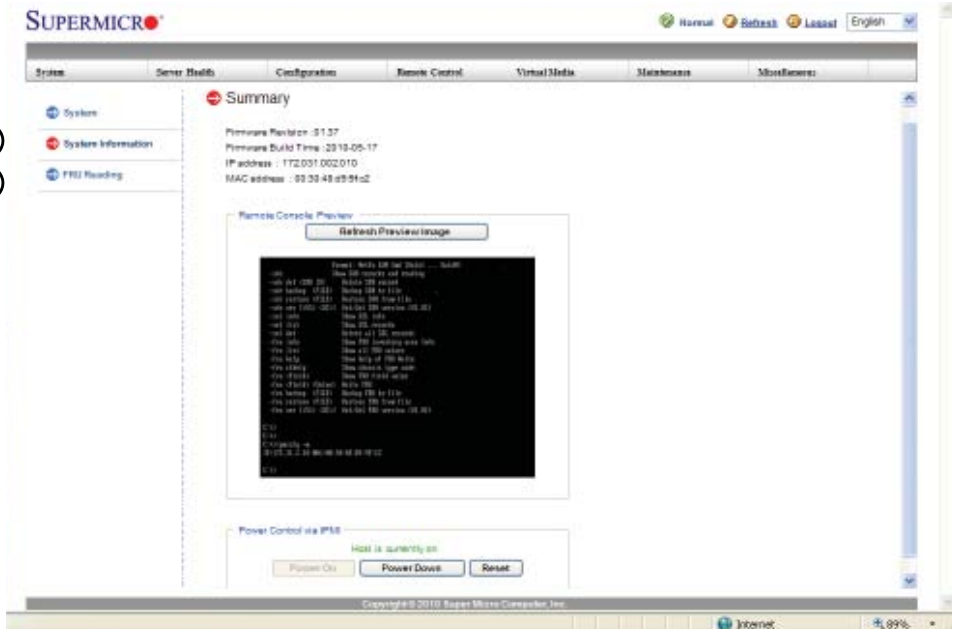
5. Language Select: From the pull-down menu, select a language.

- English

- Japanese

2.5 System Status

Once you've logged into the remote server, the IPMI Main scree will display.



1. System Information: This item displays the following firmware information.

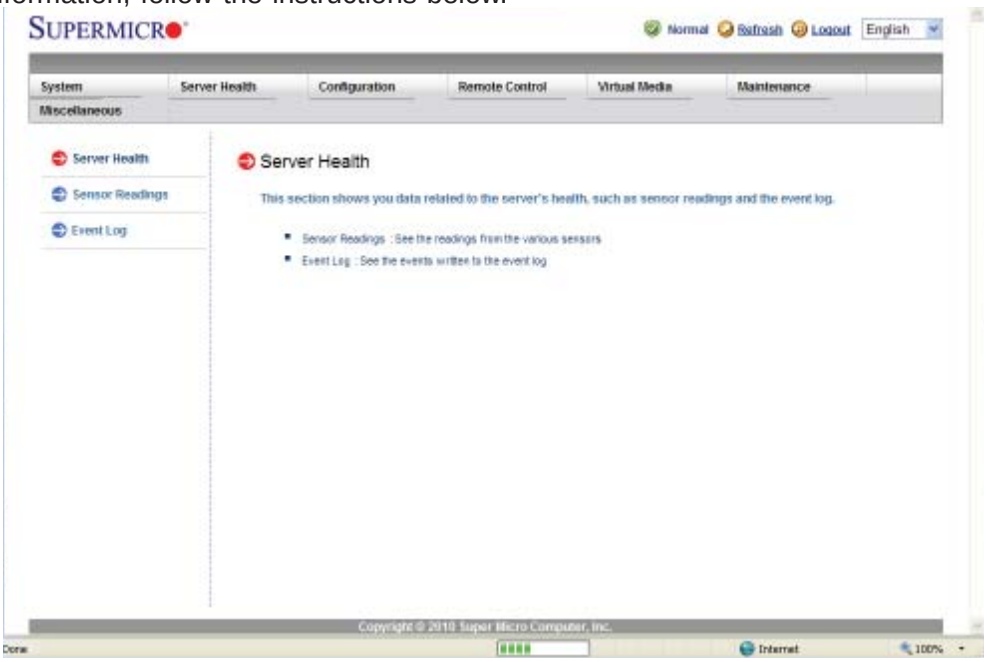
- Firmware Revision
- Firmware Build Time
- IP Address
- MAC Address
- Preview Screen
- Power Control: This feature allows the user to launch the remote console by clicking a preview screen.

2. FRU Reading: Click this item to display the following BMC FRU (Field Replaceable Unit) information. You can also configure the FRU settings by using the Supermicro IPMIView or ipmicfg utility.

- FRU Device ID
- Chassis Information
- Board Information
- Product Information

2.6 Server Health

This feature allows the user to set *Server Health* settings. To access *Server Health* information, follow the instructions below.

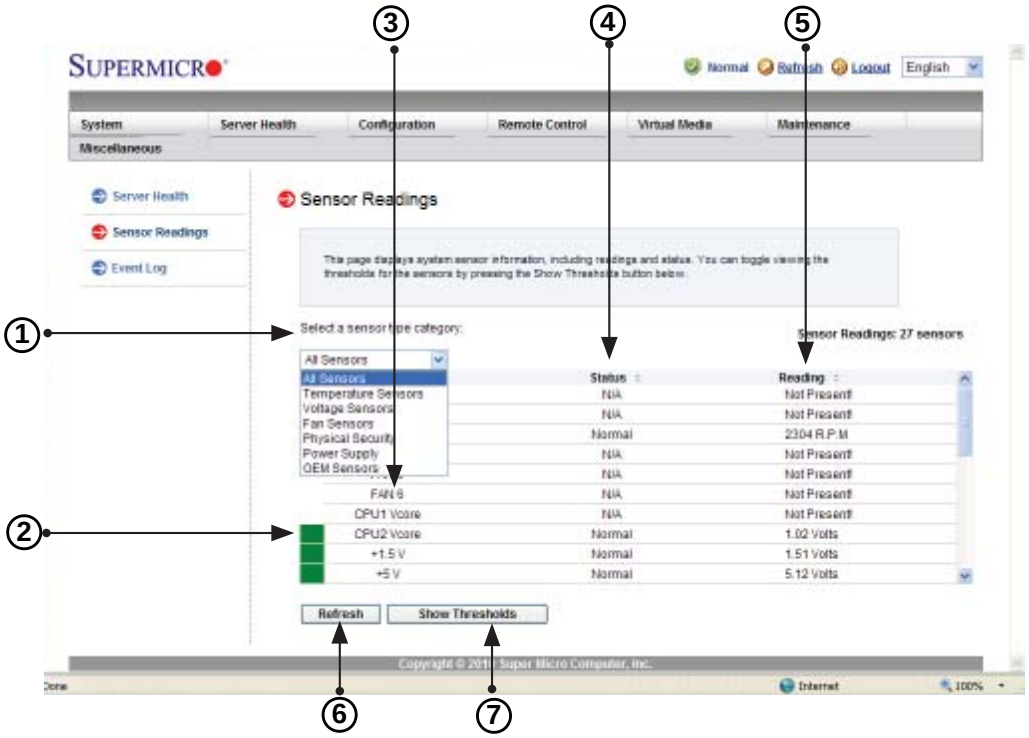


1. Click <Sensor Readings> to access information on sensor readings as shown on the next page.

2. Click <Event Log> to access event logs.

2.6.1 Sensor Readings

This page displays sensor readings for the remote console.



1. From the pull-down menu, select a sensor type (category). The options include the following.

- All Sensors
- Temperature Sensors
- Voltage Sensors
- Fan Sensors
- Physical Security/(Chassis Intrusion)
- Power Supply
- OEM Reserved:

2. A senor color that is displayed in front of an sensor indicates the status of the sensor.

- Green: It indicates that the sensor reading is normal. The system functions normally.

- Amber: There is an alert on the sensor reading. Attention is needed to ensure that the system is functioning properly.

- Red: One or more sensors have reached the critical state. Immediate action is needed to resolve the problem.

3. Name of the Sensor: This column displays the names of the sensors that are currently active in system monitoring, including system temperature, CPU temperature, fan speeds, CPU core voltages, +3.3Vcc, and +12V voltage monitoring.

4. Status: This column indicates the status of each sensor reading.

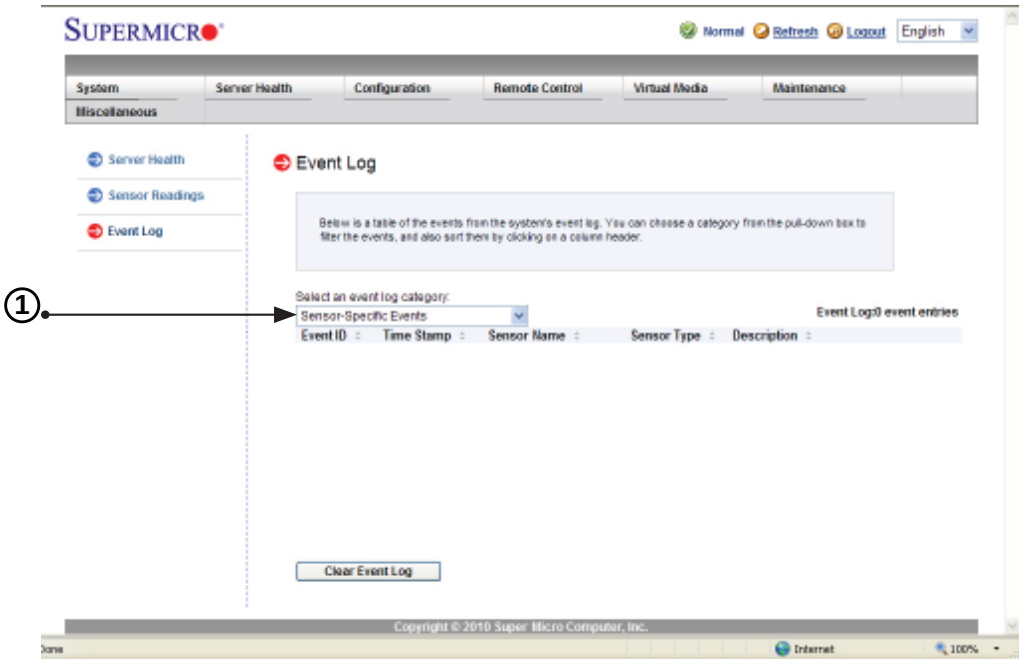
5. Reading: This column indicates the reading of each sensor.

6. Refresh: Click this item to refresh the page.

7. Show Thresholds: Click this item to display senor thresholds.

2.6.2 Event Log

This page displays a record of critical system_monitoring events. The event log indicates the time when a critical condition had occurred and when this condition was resolved. You can choose a s*pecific_event* category from the pull-down menu to display events included in this category.

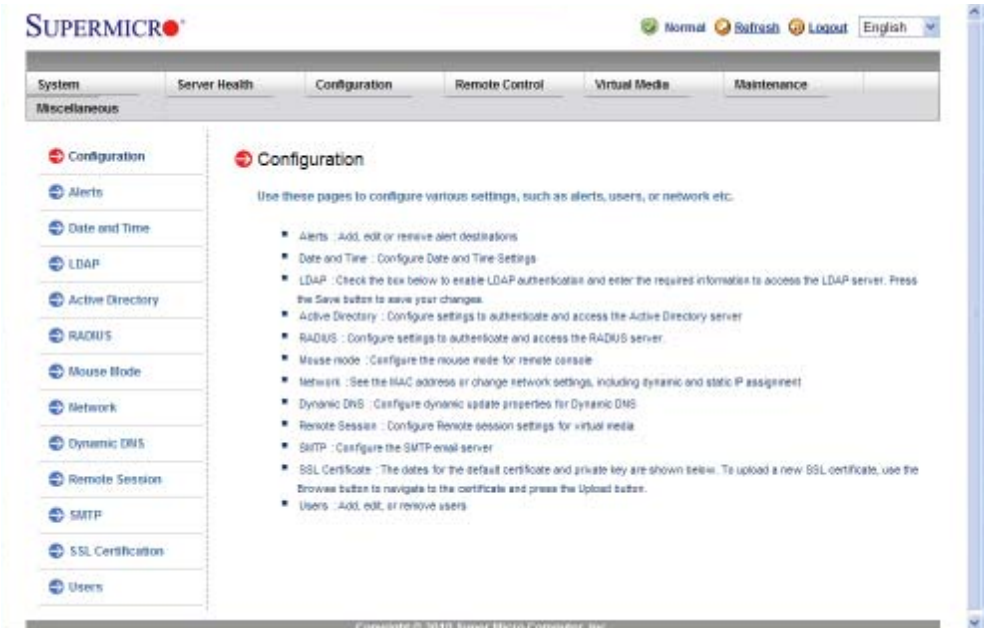


1. Event Category: From the pull-down menu, select an event category to display.

- Sensor_Specific Events
- BIOS_Generated Events
- System_Management_Software Events

2.7 Configuration

This feature allows the user to configure various network settings. When you click the *Configuration* icon on the menu bar, the following screen will display.

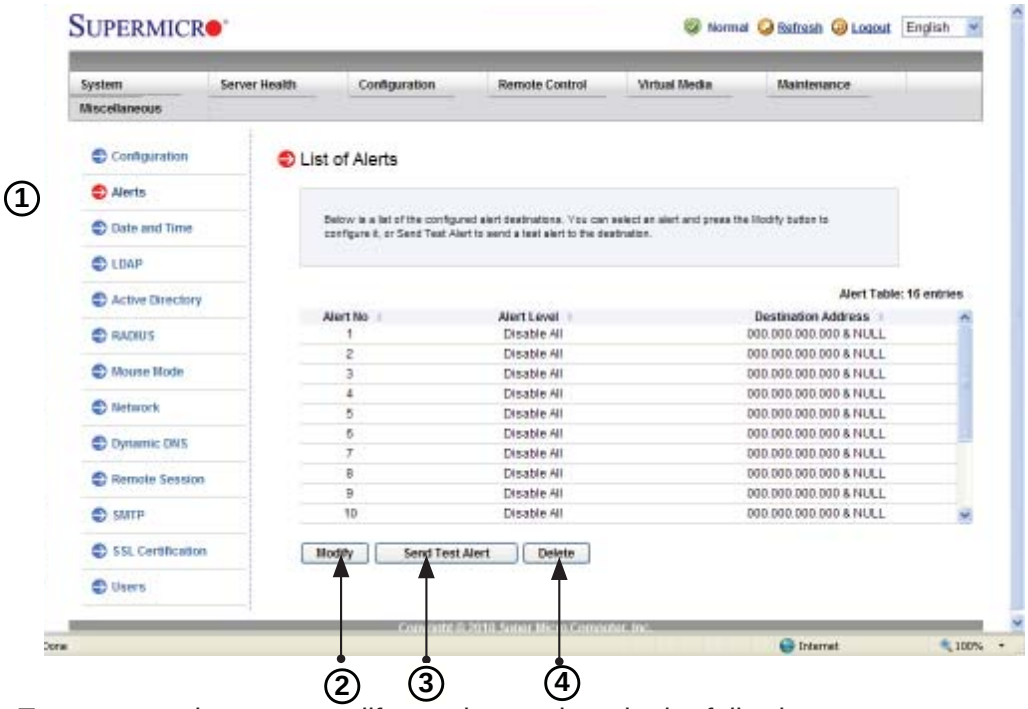

SUPERMICRO
Normal
Refresh
Logout
English
System
Server Health
Configuration
Remote Control
Virtual Media
Maintenance
Miscellaneous
Configuration
Alerts
Date and Time
LDAP
Active Directory
RADIUS
Mouse Mode
Network
Dynamic DNS
Remote Session
SMTP
SSL Certification
Users
Configuration
Use these pages to configure various settings, such as alerts, users, or network etc.
Alerts : Add, edit or remove alert destinations
Date and Time : Configure Date and Time Settings
LDAP : Check the box below to enable LDAP authentication and enter the required information to access the LDAP server. Press the Save button to save your changes.
Active Directory : Configure settings to authenticate and access the Active Directory server
RADIUS : Configure settings to authenticate and access the RADIUS server.
Mouse mode : Configure the mouse mode for remote console
Network : See the MAC address or change network settings, including dynamic and static IP assignment
Dynamic DNS : Configure dynamic update properties for Dynamic DNS
Remote Session : Configure Remote session settings for virtual media
SMTP : Configure the SMTP email server
SSL Certificate : The dates for the default certificate and private key are shown below. To upload a new SSL certificate, use the Browse button to navigate to the certificate and press the Upload button.
Users : Add, edit, or remove users

This section allows the user to configure the following settings.

- Alerts: Use this item to configure alert destination settings.
- Date & Time
- LDAP: Use this item to configure LDAP (Lightweight Directory Access Protocol) settings for authentication and access to the LDAP server.
- Active Directory: Use this item to configure the settings for authentication and access to the Active Directory server.
- Radius: Use this item to configure the settings for authentication and access to the Radius server.
- Mouse mode
- Network
- Dynamic DNS
- Remote Session
- SMTP
- SSL Certificate

2.7.1 Configuring the Alerts Settings

This feature allows the user to configure *Alert* settings. When you click the <Alerts> icon in the menu bar, the following screen will display.



To setup an alert or to modify an alert setting, do the following.

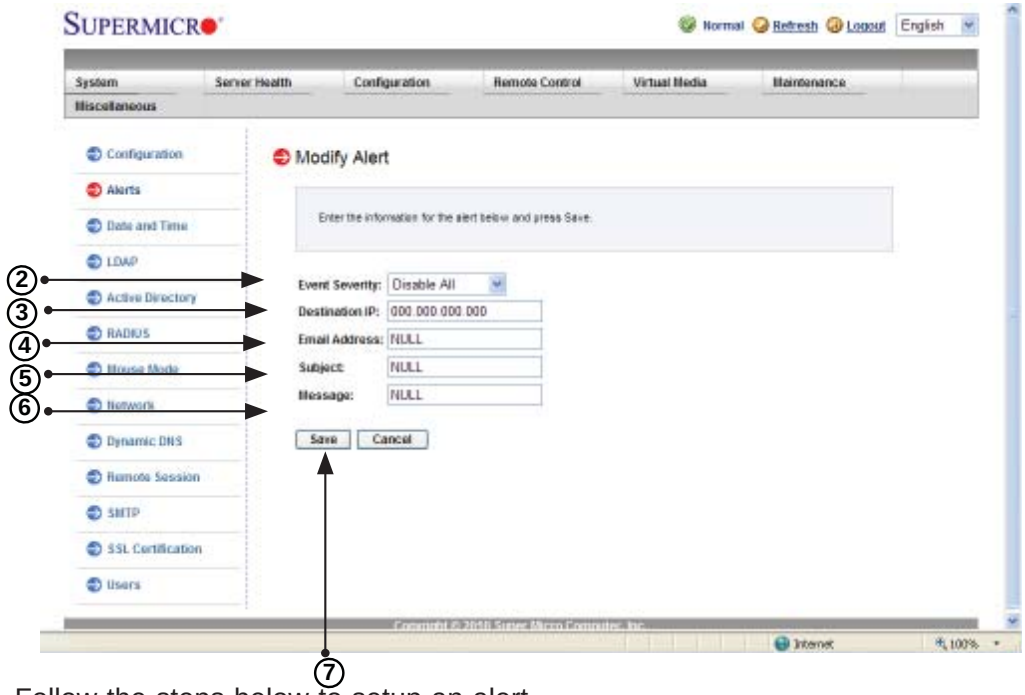
1. Click <Alerts> to activate the alert submenu.

2. Click <Modify> to configure or modify the settings of an alert.

3. *Send Test Alert* is used to check if the alerts have been set and sent out correctly.

4. Click <Delete> to delete an alert.

To Setup an Alert



Follow the steps below to setup an alert.

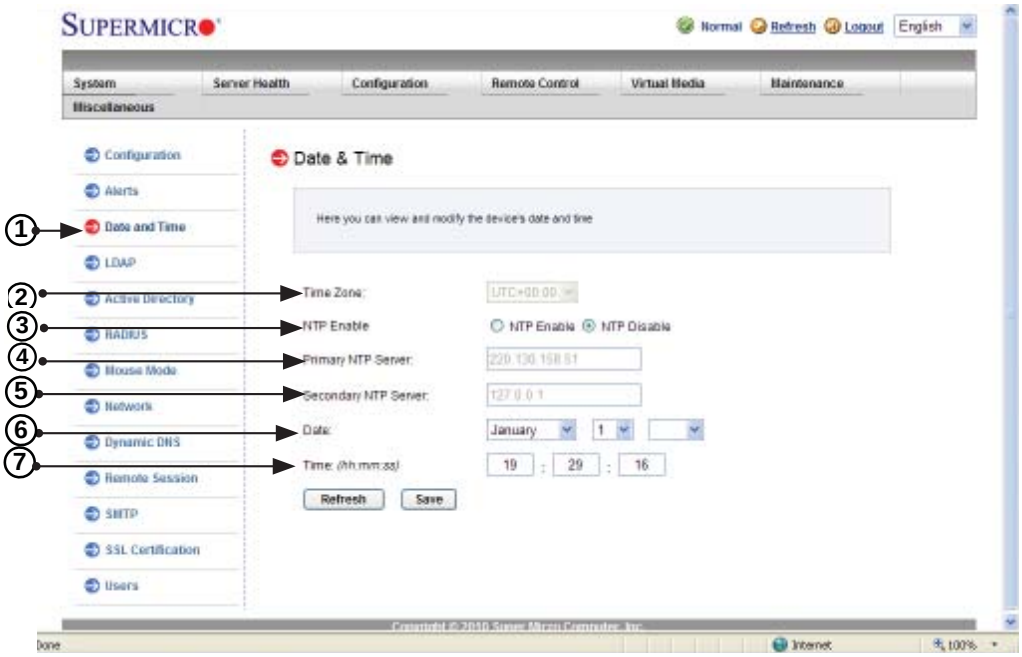
1. Select *Alert Severity*.

2. Enter the IP address and/or the email address to receive the SNMP Trap.

3. Enter a subject or a message if applicable.

2.7.2 Configuring Date and Time Settings

This feature allows the user to configure the time and date settings for the host server and the client computer. When you click the <Time and Date> icon in the Options window, the following screen will display.

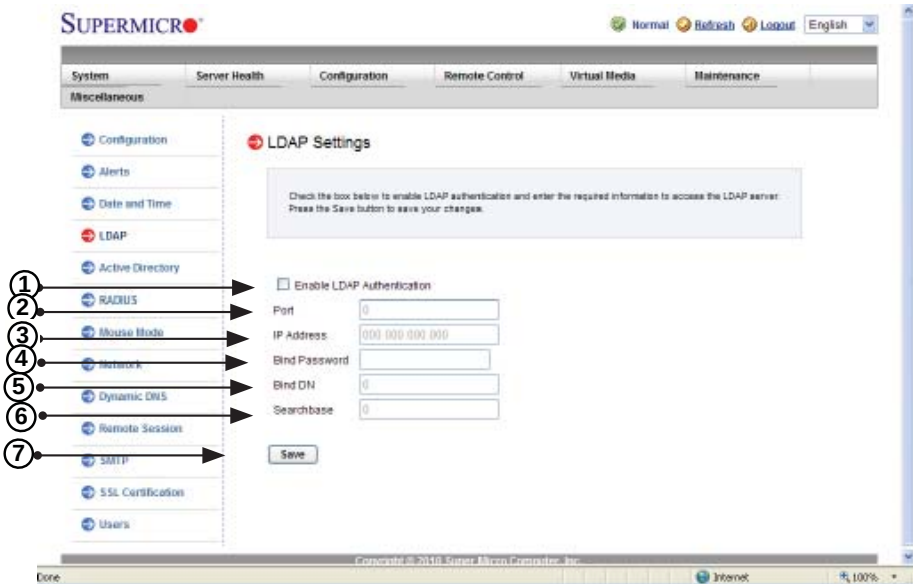


The user can either set the date & time setting manually or use the *NTP Server* setting to set date & time.

> **Note**: Time zone is enabled when *NTP* is selected. The options are UTC -12:00 hr. ~ +12:00 hr.

2.7.3 Configuring the Light-Weight Directory Access Protocol (LDAP) Settings

This feature allows the user to configure the *Light-Weight Directory Access Protocol* (LDAP) settings. When you click <LDAP> in the Options window, the following screen will display.



Follow the steps below to configure the LDAP settings.

1. Check the enable box to enable *LDAP Authentication* support.

2. Enter a port number for the LDAP server.

3. Enter an IP Address for the LDAP server.

4. Enter a Bind Password for the LDAP server.

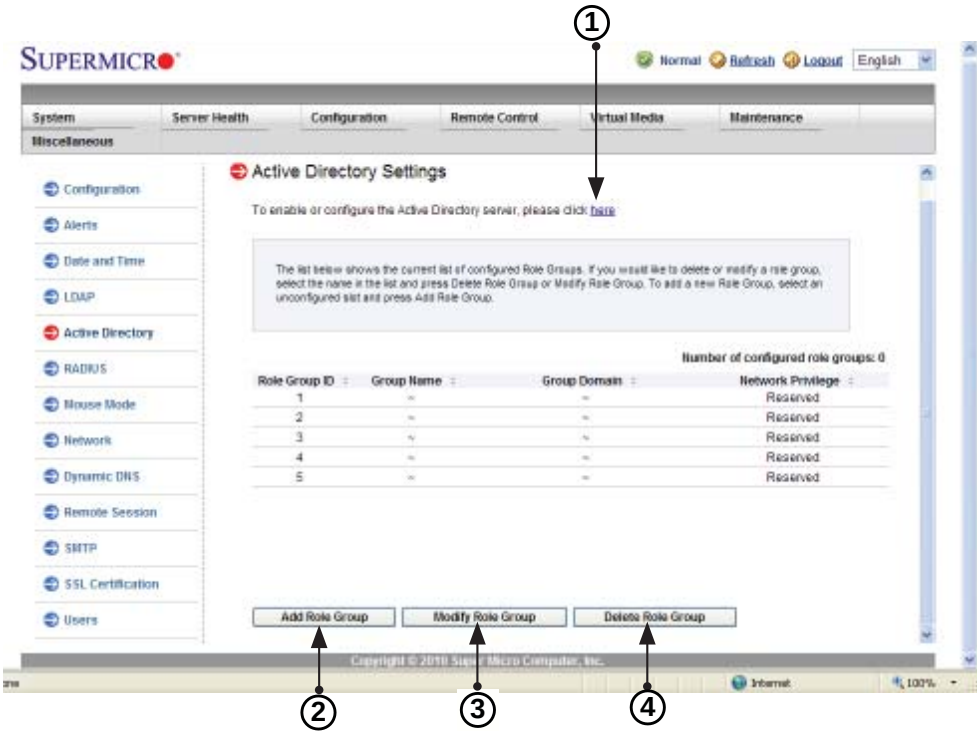
5. Enter a Bind DN value in the field. (The bind DN is the user or the LDAP server that is permitted to do search in the LDAP directory within a defined search base.)

6. Enter a SearchBase value in the field. (The SearchBase is the directory that allows the external user to search data.)

7. After entering the information in the fields, click <Save> to save the information you've entered.

2.7.4 Active Directory Settings

This page displays a list of role groups and their Group IDs, Group Names, Domains and Network Privilege settings. When you click the <Active Directory> icon in the Options window, the following screen will display.



1. Click <HERE> to enable or configure the Active Directory server. See the next page for enabling or configuring Active Directory instructions.

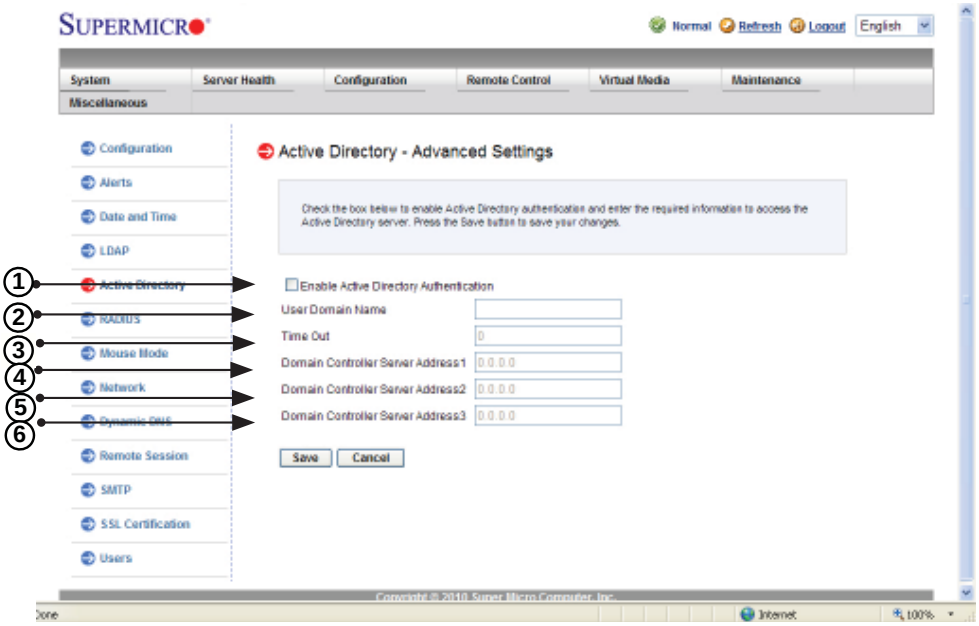
2. Select a group and click <Add> to add a role group.

3. Select a group and click <Modify> to modify a role group.

4. Select a group and click <Delete> to delete a role group.

Configuring the Active Directory Settings

This feature allows the user to configure the *Advanced Active Directory* settings. When you click <Here> on the screen shown on the previous page, the following screen will display.



1. Check the <Enable> box to enable *Active Directory* authentication support. Then, Enter the values in the fields below.

2. Enter User Domain Name in the field.

3. Enter Time_Out value in the field to set the time limit for a user to stay logging-in.

4. Enter <Controller Server Address1>.

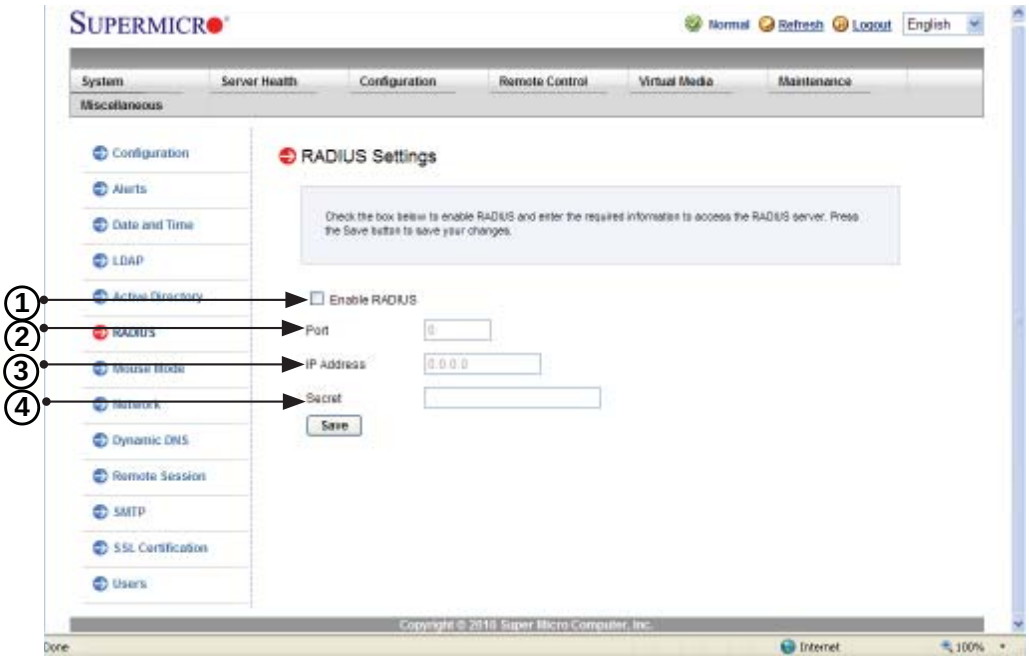
5. Enter <Controller Server Address2>.

6. Enter <Controller Server Address3>.

After entering the information, click <Save> to save the settings.

2.7.5 Configuring the Radius Settings

This feature allows the user to configure *Radius Option* settings. When you click <Radius>in the Options Window, the following screen will display.



1. Check the <Enable> box to enable *Radius* support. Enter the information in the fields below to configure *Radius* settings.

2. Enter the port number for the Radius server.

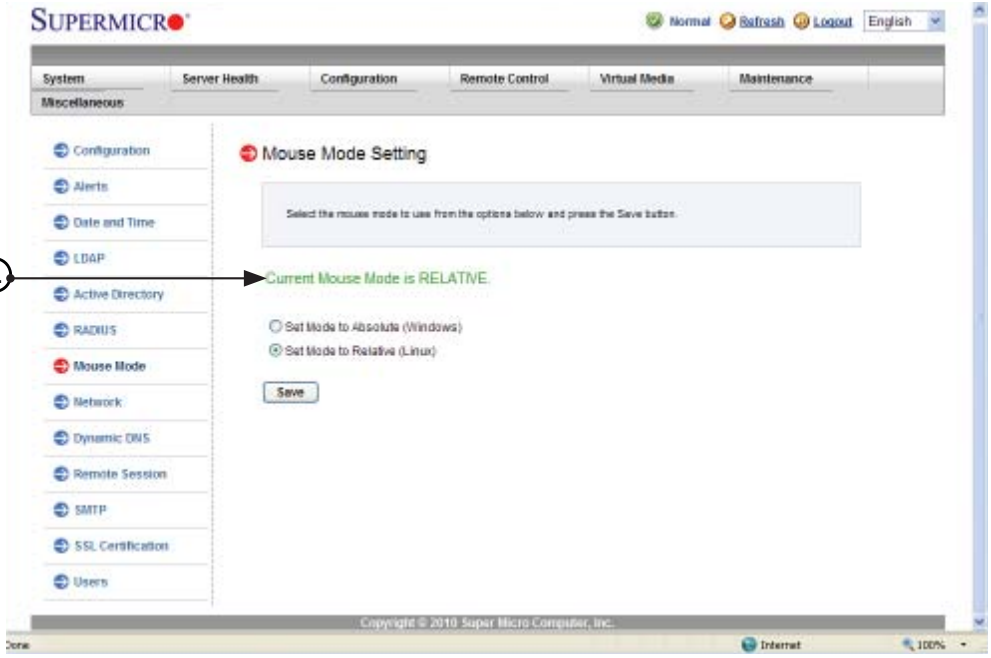
3. Enter the IP address of the Radius server.

4. Enter a (secret) password for the user to access the Radius server

After entering the information in the fields, click <Save> to save the information you've entered.

2.7.6 Configuring the Mouse Mode Settings

This feature allows the user to configure the *Mouse_Mode* settings. When you click the <Mouse Mode> icon in the Options Window, the following screen will display.



1. This item displays the current Mouse_Mode setting. To select a proper Mouse_Mode setting, click the proper radio button as shown below.

- Check the radio button to set the mouse mode to *Absolute Mode* for the Windows OS. (This is the default setting.)

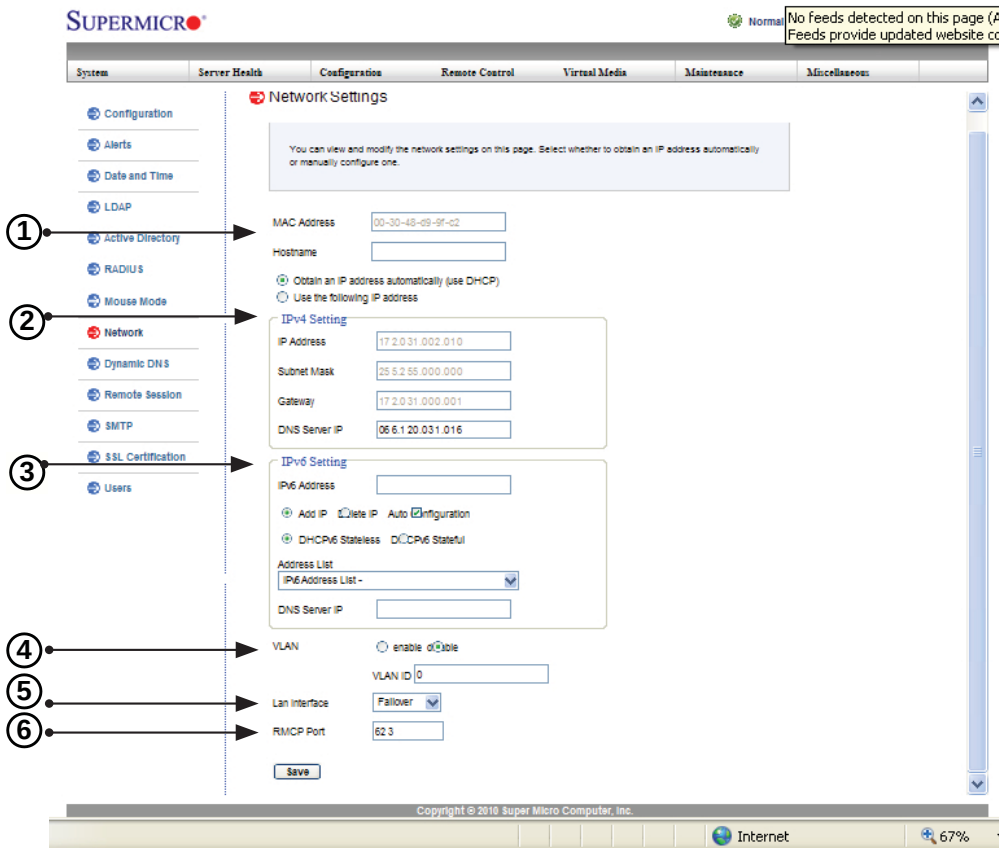
- Check the radio button to set the mouse mode to *Relative Mode* for the Linux/ Unix OS.

After entering the information, click "Save" to save the settings.

Note: IPMI is an OS-independent platform, and IKVM support is an added feature for IPMI. For your mouse to function properly, please configure the Mouse_Mode settings (see above) according to the type of OS used in your machine.

2.7.7 Configuring Network Settings

This feature allows you to configure the network settings. When you click the <Network> icon in the Options Window, the following screen will display.



To configure *Network* settings, follow the instructions below.

1. Enter the MAC address for the network server. You can also check the first radio button to obtain an IP address automatically by using DHCP (Dynamic Host Configuration Protocol) or check the second radio button to setup the IP address by manually entering the information in the fields below. (**Note**: DHCP is the default setting.)

2. To set the IP address using the IPv4 format, enter proper information in the following fields.

- IP address
- Subnet Mask Default Gateway
- DNS Server IP

3. To set the IP address using the IPv6 format, enter an IPv6 Address in the field and enter proper information in the related fields.

4. Check this box to enable Virtual LAN support, and enter the VLAN ID in the field.

5. LAN Interface

This feature allows the user to select the port to be used for IPMI out-of-band communication.

- The default setting is Failover, which will allow IPMI to be connected from either the shared LAN port (LAN1/0) or the dedicated IPMI LAN port. Precedence is given to the Dedicated LAN port over the shared LAN port.

- Select <Dedicated LAN> for IPMI to connect through the IPMI Dedicated LAN port at all time.

- Select *Shared LAN* for IPMI to connect through the LAN port on the board.

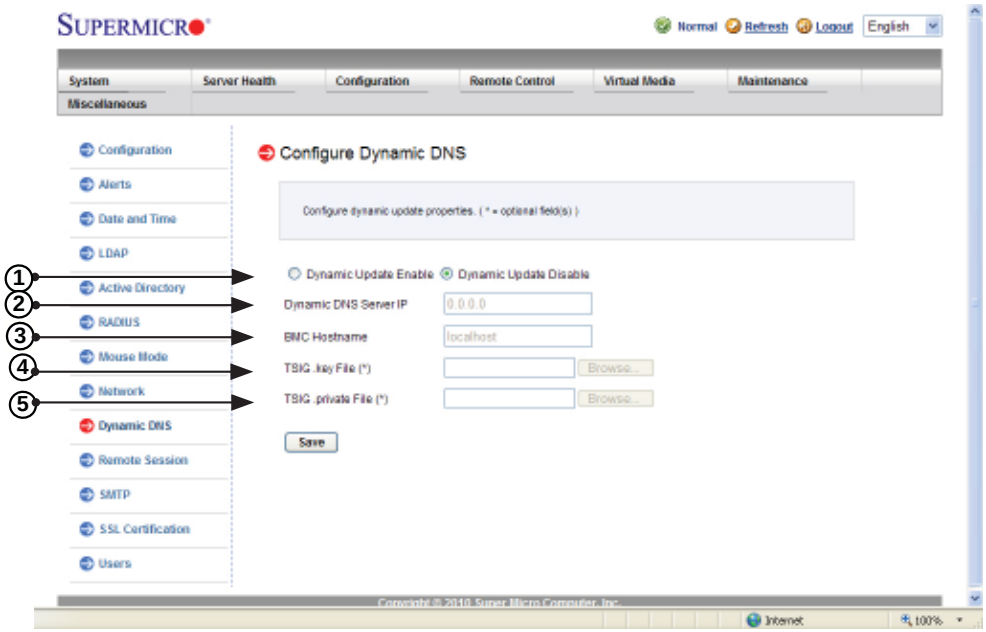
6. RMCP Port

This feature allows the user to select the desired RMCP (Remote Mail Checking Protocol) port based on his configuration. The default port is 623.

After entering all fields above, click <Save> to save the Network settings.

2.7.8 Configuring Dynamic DNS (Domain Name System) Settings

This feature allows you to configure DNS settings. When you click the Dynamic DNS icon in the Options Window, the following screen will display.



1. Click the <Enable> radio button to enable Dynamic DNS update support. Click Disable to disable Dynamic DNS update support. (**Default**: Disable)

2. Enter the IP address of your Dynamic DNS (Domain Name System) server.

3. Enter the name of the BMC (Baseboard Management Controller) Host Server.

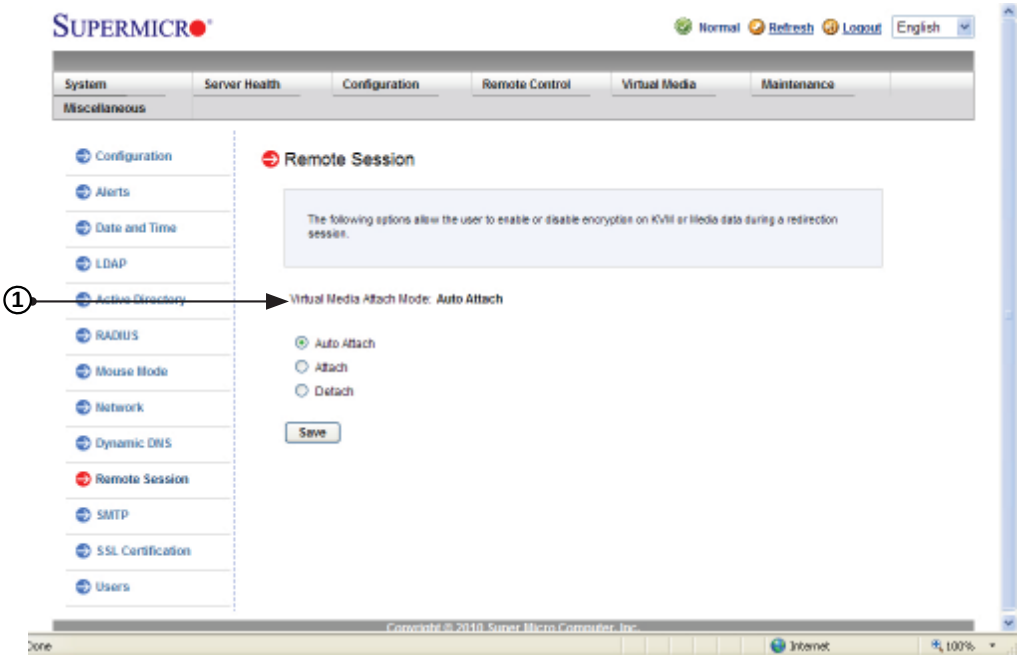
4. Browse the files to select the *TSIG.key* file. (This item is optional.)

5. Browse the files to select the *TSIG.private* file. (This item is optional.)

After entering the required information in the fields, click <Save> to save the information you have entered.

2.7.9 Configuring the Remote Session Settings

This feature allows the user to enable or disable encryption support on IKVM, or to select the Virtual_Media_Attach mode for console redirection. When you click the Remote Session in the menu bar, the following screen displays.



1. This item displays the current Virtual_Media_Attached mode. To change the Virtual_Media_Attached mode, select the desired setting from the list below.

- Auto_Attach (Default): Select this mode to automatically enable virtual media support and make it available for remote access. Virtual devices will only be shown in the operating systems and the BIOS when a device or an ISO image is connected through the virtual media wizard.

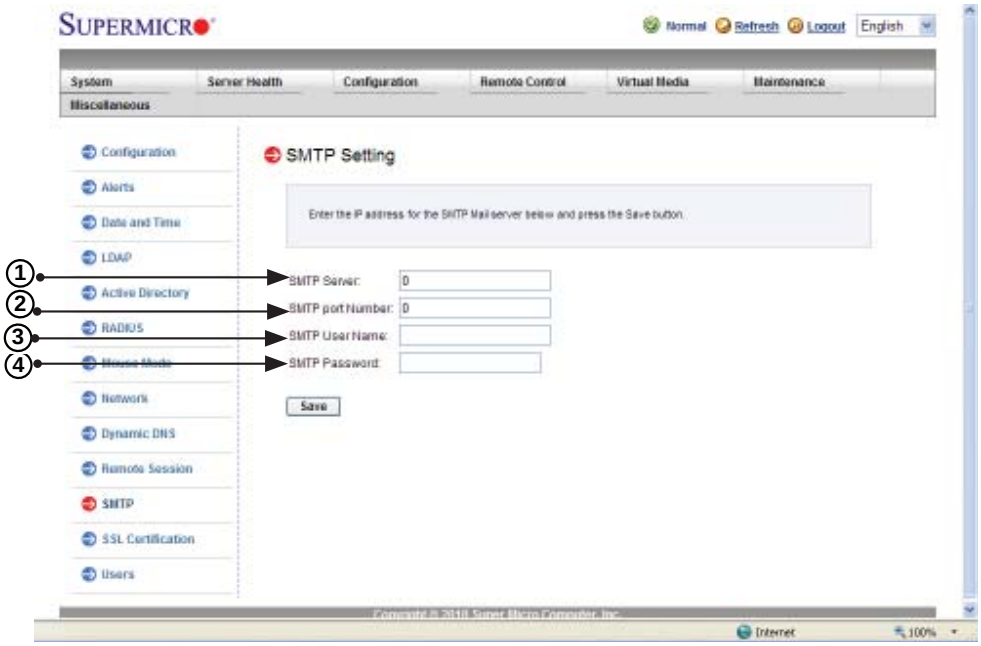
- Attach: Select this mode to activate a virtual media and make it available for remote access. A virtual device will always be seen in the system BIOS even when it is not active.

- Detach: Select this mode to disable virtual media for remote access.

After making selection, click <Save> to save the settings.

2.7.10 Configuring the SMTP Settings

This feature allows the user to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network. When you click the <SMTP> icon in the Options window, the following screen will display.



To configure SMTP settings, enter information in the fields below.

1. Enter the IP address for the SMTP (Simple Mail Transfer Protocol) Mail server.

2. Enter the port number for your SMTP Mail server.

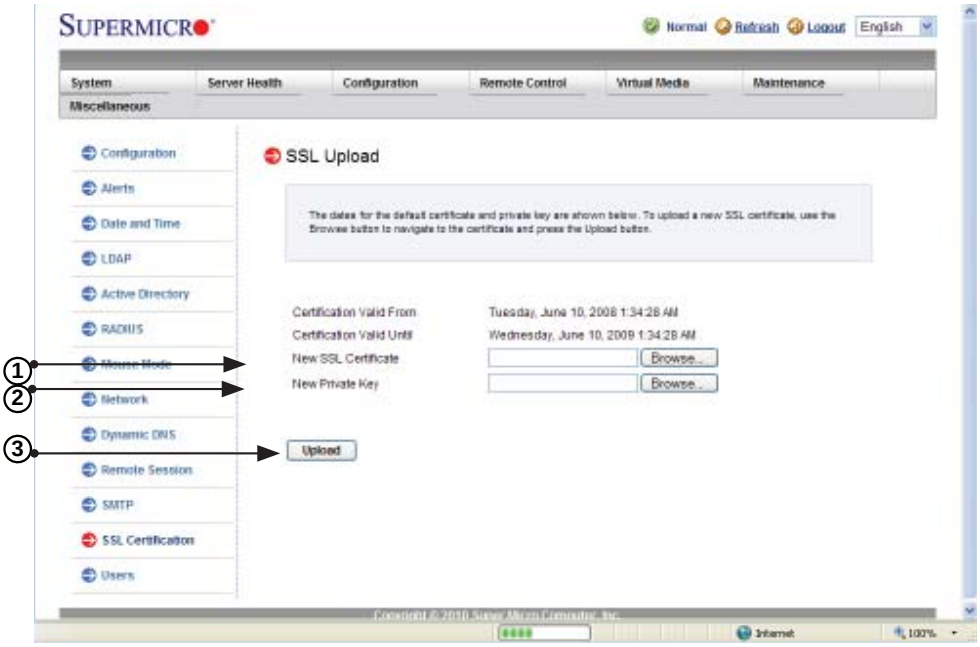
3. Enter the user name for your SMTP Mail server. (Optional)

4. Enter the user password for your SMTP Mail server. (Optional)

After entering the information above, click <Save> to save the settings.

2.7.11 Configuring the SSL (Secure Sockets Layer) Certification

This feature displays the default certificate and private keys. It also allows the user to upload a new SSL certificate. When you click the <SSL> icon in the Options window, the following screen will display.



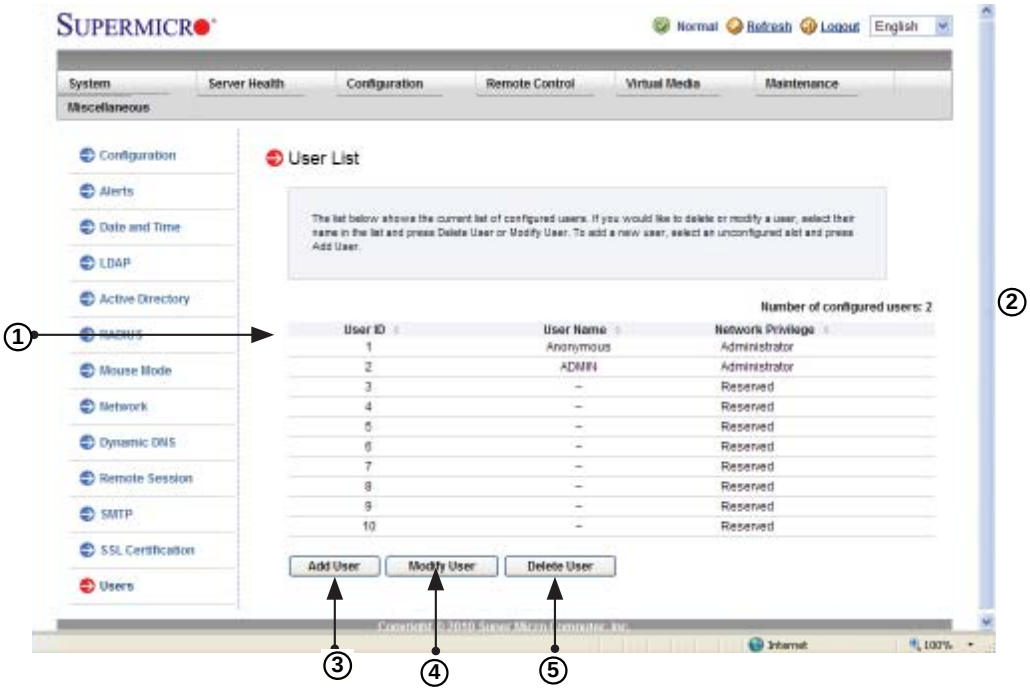
1. To enter a new SSL Certificate, enter a new certificate in the field. You can also browse the data base to select a new certificate.

2. Enter a new Private Key in the field, if desired. You can also browse the data base to select a new key.

3. After entering the new SSL certificate or/and a new private key, press <Upload> to upload the certificate and private key to the server.

2.7.12 Configuring Users Settings

This page displays information on the current users. It also allows you to add, delete or modify user information. When you click the <Users> icon in the Options window, the following screen will display.



1. This item lists current user information, including User ID, User name and Network Privilege settings. Network privilege settings are shown below.

Privilege Levels Defined

Function	User	Operator	Administrator
System Information	Full Access	Full Access	Full Access
Chassis Locator Control	View Only	Full Access	Full Access
FRU Reading	Full Access	Full Access	Full Access
Sensor Readings	Full Access	Full Access	Full Access
Event Log	View Only	Full Access	Full Access
Alert	No	View Only	Full Access
LDAP	No	View Only	Full Access
Mouse Mode	No	View Only	Full Access
Network	No	View Only	Full Access
Remote Session	No	View Only	Full Access
SMTP	No	View Only	Full Access
SSL	No	View Only	Full Access
Users	No	View Only	Full Access
Event Action	No	View Only	Full Access
Power Control	View Only	Full Access	Full Access
KVM	View Only	Full Access	Full Access
F/W update	View Only	View Only	Full Access
SDR update	View Only	View Only	Full Access
Logout	Full Access	Full Access	Full Access

2. This item displays the number of the users that are set up for the network. The maximum of 10 user profiles can be made.

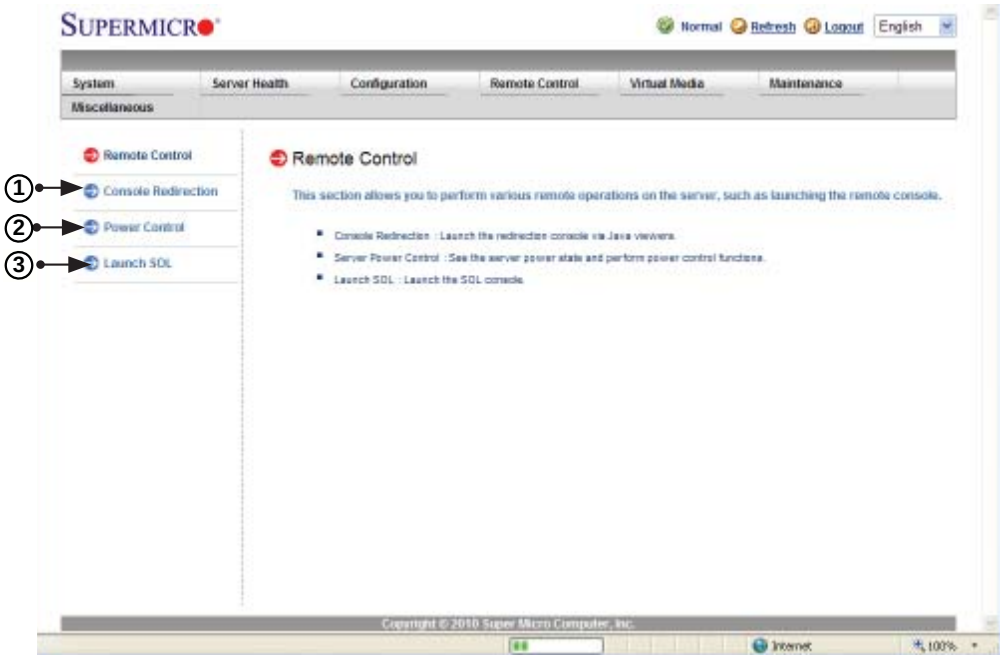
3. To add a new user to the network, click <Add User>. When prompted, select an empty slot from the users list to add an user.

4. To modify the information or the status of a user, click <Modify User>. When prompted, using the arrow keys, select a user from the users list to modify the user information.

5. To delete a user from the network, click <Delete User>. When prompted, using the arrow keys, select a user from the users list to delete it from the list.

2.8 Remote Control

This section allows the user to carry out activities and perform operations on a remote server via remote access.



To launch remote console or to change to power settings of the remote console, follow the instructions below.

1. Click "(Launch) Console Redirection" to launch Console Redirection and configure the settings of the remote server. For more details on Console Redirection, please refer to "Launching Console Redirection" on the next page.

2. Click "Power Control" to display and configure the power settings of the remote console, including the following settings.

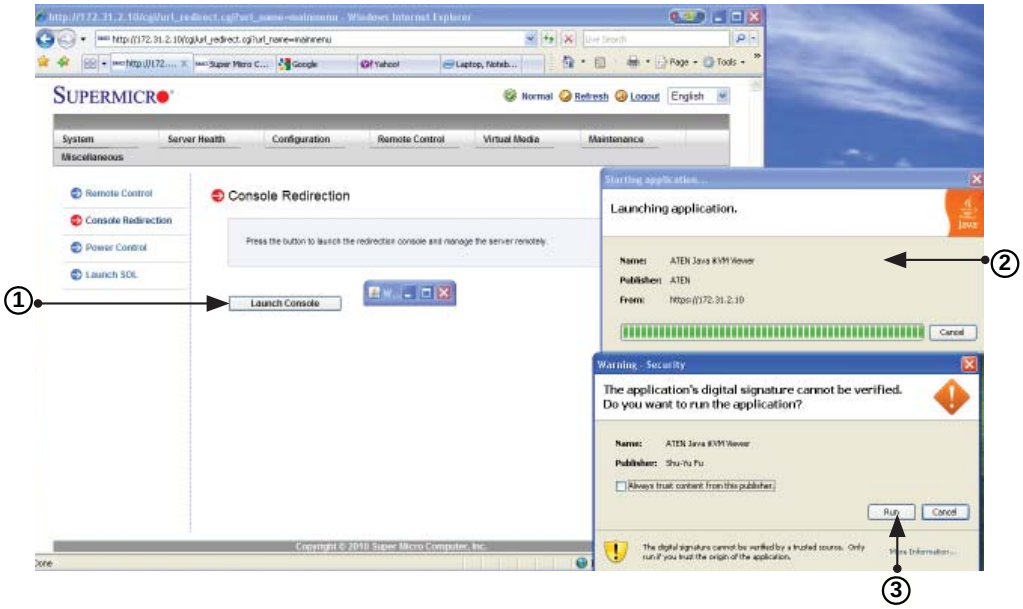
- Reset Server
- Power Off Server-Immediately
- Power Off Server-Orderly Shutdown
- Power On Server
- Power Cycle Server

Once you have clicked the desired power setting, click "Perform Action" to change the power setting of the server.

3. Click "Launch SOL" to launch SOL (Serial_Over_LAN) console and manage the remote server.

2.8.1 Launching Console Redirection

This feature allows you to launch Console Redirection via IKVM (keyboard, video/ monitor, mouse) support. When you click <(Launch) Console Redirection> in the Options window, the following screen will display.



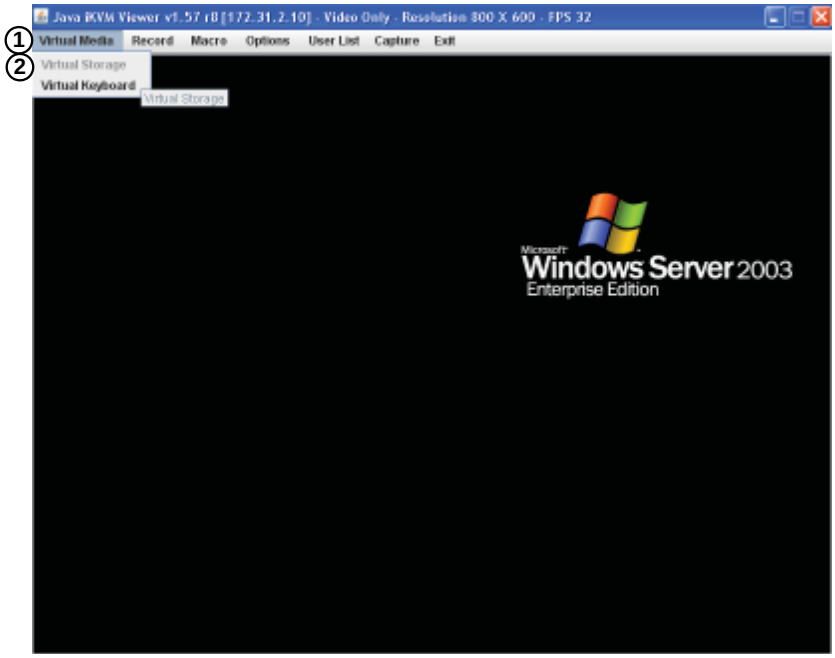
1. Click <Launch Console> on the Console Redirection screen to launch the remote console via Java or Active X (for the Internet Explorer). If it is blocked by the IE due to security reasons, click on the top of the menu bar and select <Download File>.

2. A screen will display to indicate that Java is launching.

3. When the warning screen as shown above displays, click <Run> to launch the remote console.

2.8.1.1 Console Redirection - Virtual Device

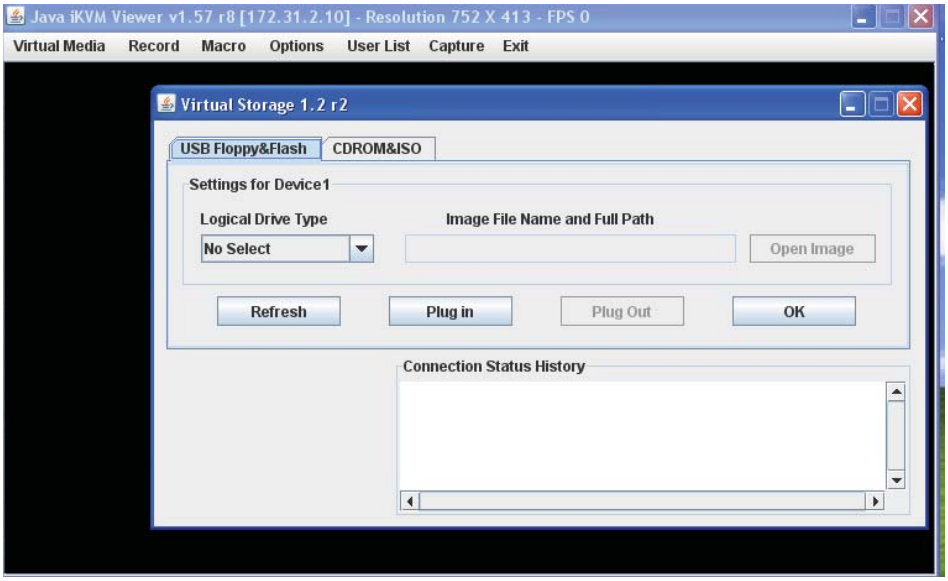
This feature allows you to configure Virtual Device settings for your console redirection. When you click the <Virtual Device> icon in the Menu bar, the video settings of the remote console will display as shown below.



1. Click <Virtual Media> to configure virtual device settings of a server at a remote site via Console Redirection.

2. Click <Virtual Storage> to select a device you want to connect to the remote server as a virtual device. When you click on this item, the screen as shown below displays.

You can connect Floppy, USB Flash, CD-ROM, DVD ROM or ISO images using this feature.



Virtual Keyboard

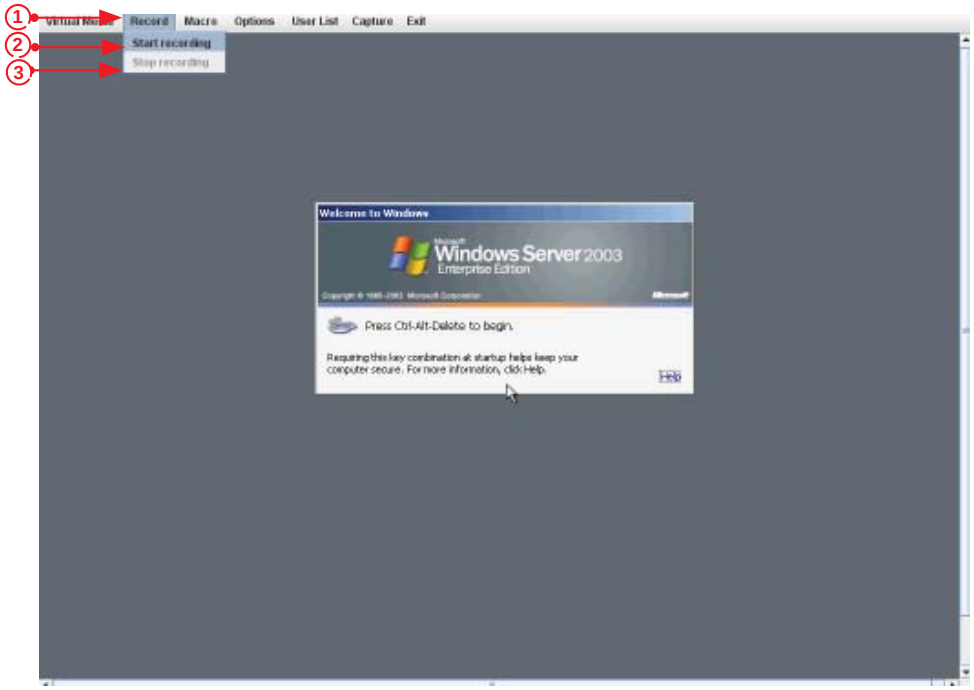
1. Click the <Virtual Keyboard> to use the on_screen Keyboard.

2. The screen above shows the Virtual Keyboard in English. Click a key on the keyboard for your BMC connection.

①
②
English keyboard
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 psc slk pau
` 1 2 3 4 5 6 7 8 9 0 - = ins nlk / * -
q w e r t y u i o p [ ] \ del
a s d f g h j k l ; '
z x c v b n m , . /
ctrl alt alt ctrl
ins del
+

2.8.1.2. Console Redirection - Recording

This feature allows you to record media displays for your console redirection. When you click the Record icon in the Menu bar, Record settings will be shown below.



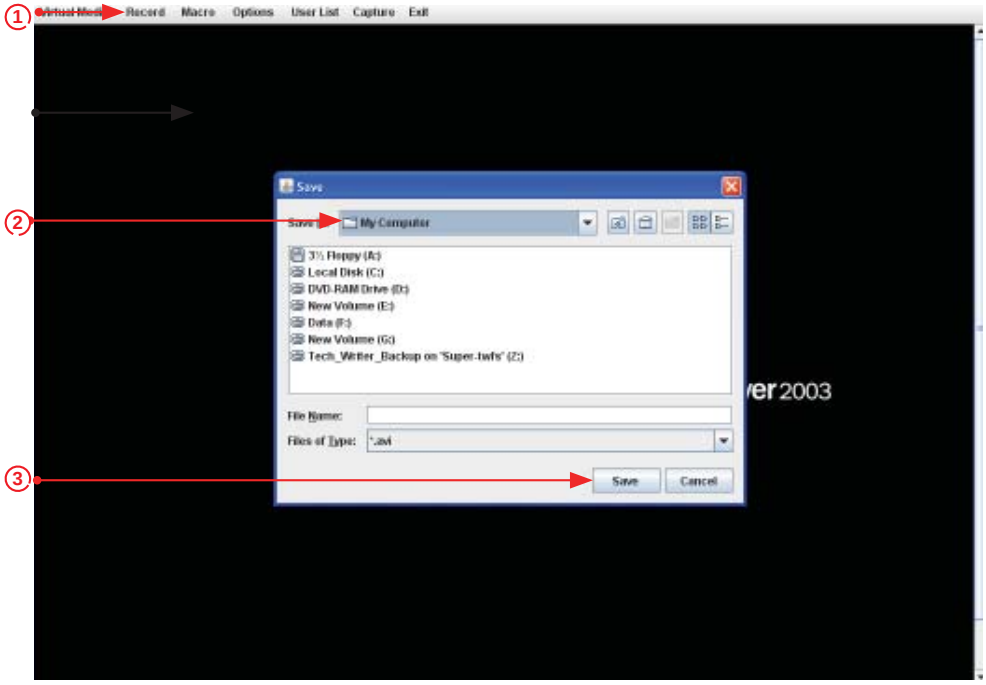
1. Click <Record> to use the recording features for your remote server. The features include the following.

2. Click <Start Recording> to start video recording from your remote server.

3. Click <Stop Recording> to stop video recording from your remote server.

2.8.1.3. Console Redirection - Recording

This feature allows you to record the media displays. Click <Record> in the Menu bar to enable virtual media recording support.



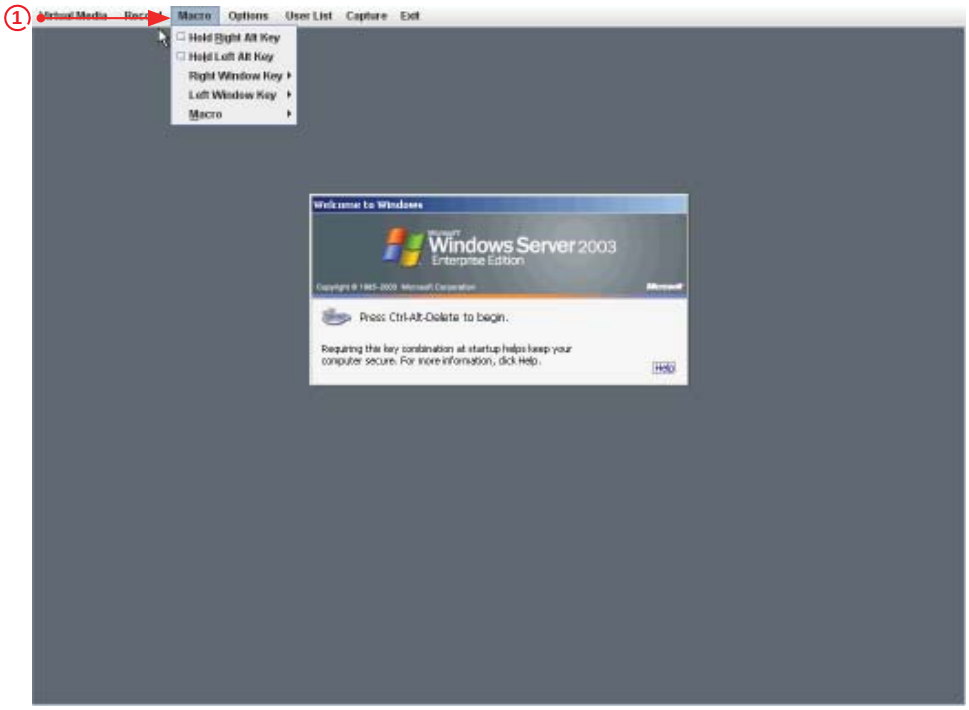
1. Click <Record> to enable media recording support. Click <Start Recording> to start recording.

2. From the pull-down menu, select the location where you want to save the recording.

3. Enter the filename and click <Save> to save the recording.

2.8.1.4. Console Redirection - Macro

This feature allows you to configure Macro settings for your console redirection. When you click the <Macro> icon in the Menu bar, the macro settings screen will display as shown below.



Click <Macro> to configure the Macro settings for your remote server. The features include the following.

- **Hold Right_ALT Key:** This item performs the same function as holding down the <Right_Alt> key.

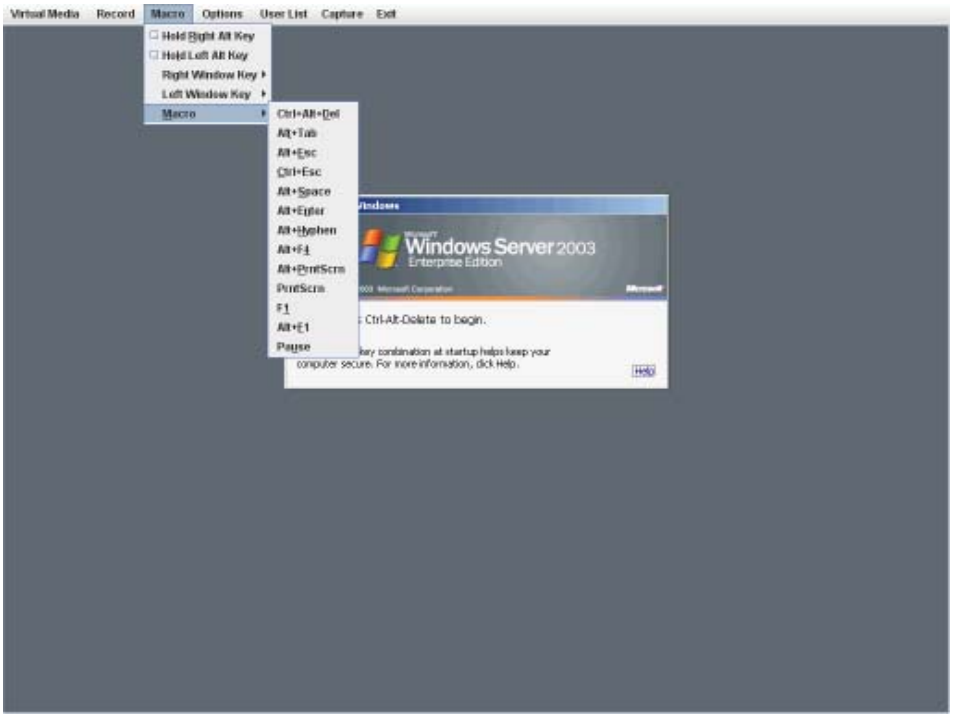
- **Hold Left_ALT Key:** This item performs the same function as holding down the <Left_Alt> key.

- **Right_Windows Key:** This item performs the same function as you pressing the <Right_Windows> key. Right click this item to select <Hold Down> or <Press & Release> for the Right_Windows key.

- **Left_Windows Key:** This item performs the same function as pressing the <Left_Windows> key. Right click this item to select <Press Down> or <Press & Release> for the <Left_Windows> key.

- **Macro:** Click this item to activate a pull-down submenu. The Macro_Hotkey submenu includes the following items as shown on the next page.

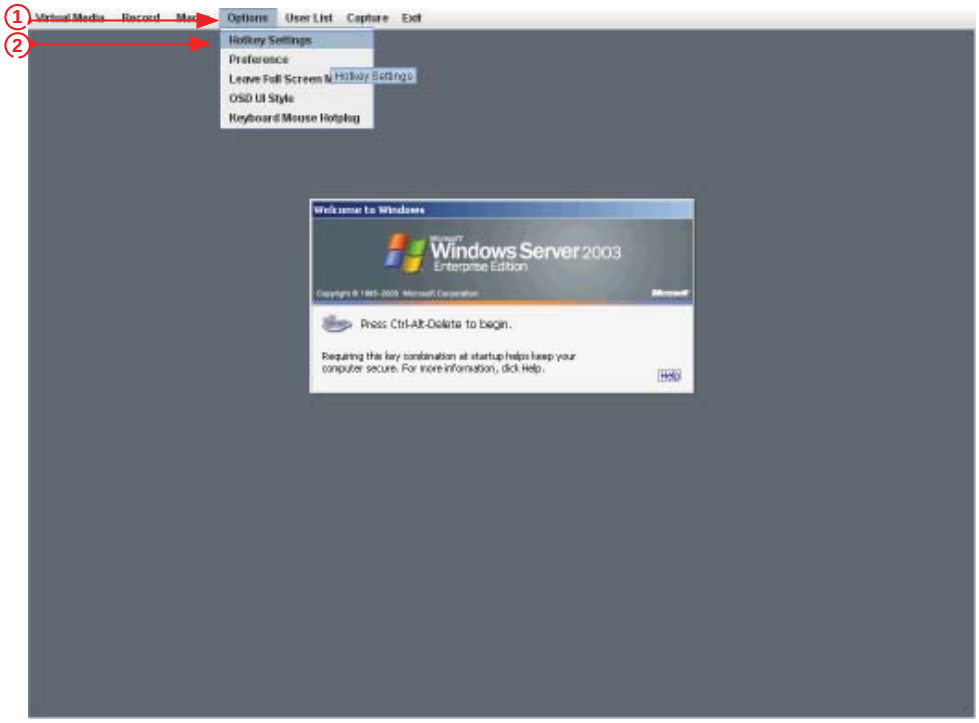
Click <Macro Hotkeys> to display the Macro_Hotkey pop-up submenu. The hot keys include the following:



- CTRL + ALT + Del
- ALT + Tab
- ALT + Esc
- Ctrl + Esc
- ALT + Space
- ALT + Enter
- ALT + Hyphen
- ALT + F4
- ALT + Prnt Scrn
- Prnt Scrn
- F1
- Alt + F1
- Pause

2.8.1.5 Console Redirection - Options

This feature allows you to configure *Options* settings for your console redirection. When you click the <Options> icon in the Menu bar, the Options menu will display as shown below.



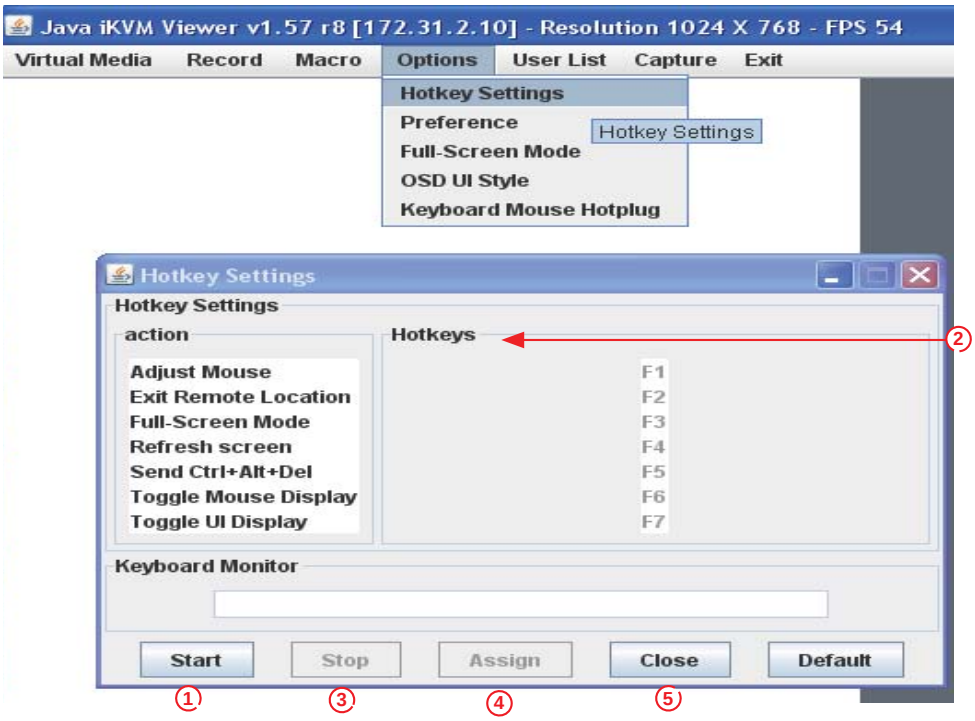
1. Click <Options> to activate the pull-down menu to configure *Options* settings.

2. The options menu allows you to configure the following settings.

- Hotkey
- Preference
- Full-Screen Mode
- OSD UI Style
- Keyboard_Mouse_Hotplug

2.8.1.5.1 Console Redirection - Options: Hotkey Settings

This feature allows you to configure Hotkey settings for your console redirection. When you click the <Options-Hotkey> icon in the Menu bar, the Hotkey menu will display as shown below.

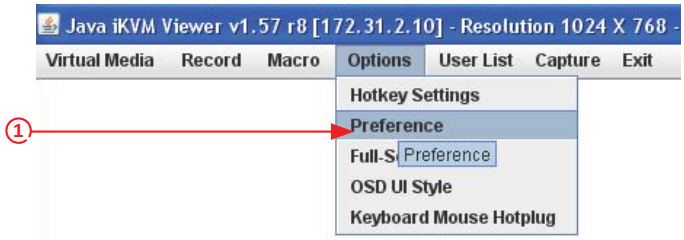


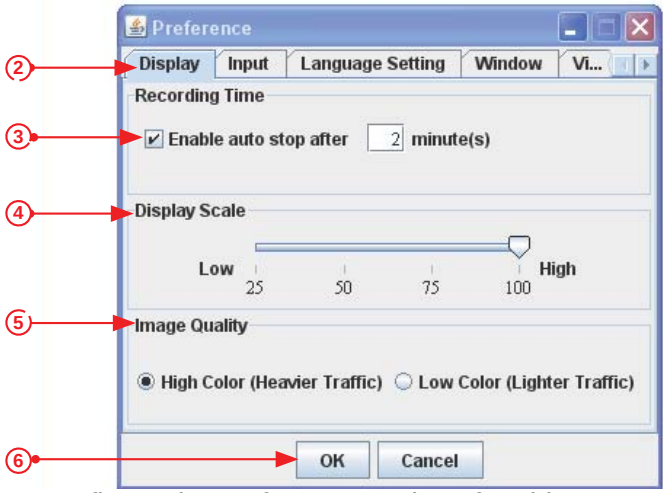
To assign a hotkey for an action, follow the steps below.

1. Click <Start>.
2. Enter the hotkey of your choice (-it can be a single word or a combination).
3. Click <Stop>.
4. Select an item from the action list and click <Assign>.
5. Click <Close> to exit.

2.8.1.5.2. Console Redirection - Options: Preference (-Display)

This feature allows you to configure Video Recording Preference settings for your console redirection. When you click the <Preference> icon in the Menu bar, the Preference menu will display as shown below.





To configure the preference settings for video recording, please follow the instructions below.

1. Click <Preference> to invoke the Preference submenu which includes Display, Input, Language Setting, Window and Video Stream Control settings.

2. Click <Display> to configure Video Display features.

3. Check this box to enable Auto_Stop support, which will allow the video recording to be automatically turned off after recording of certain period of time. After <Enable auto_stop> is checked, enter the number of minutes upon which your video recording will be automatically turned-off.

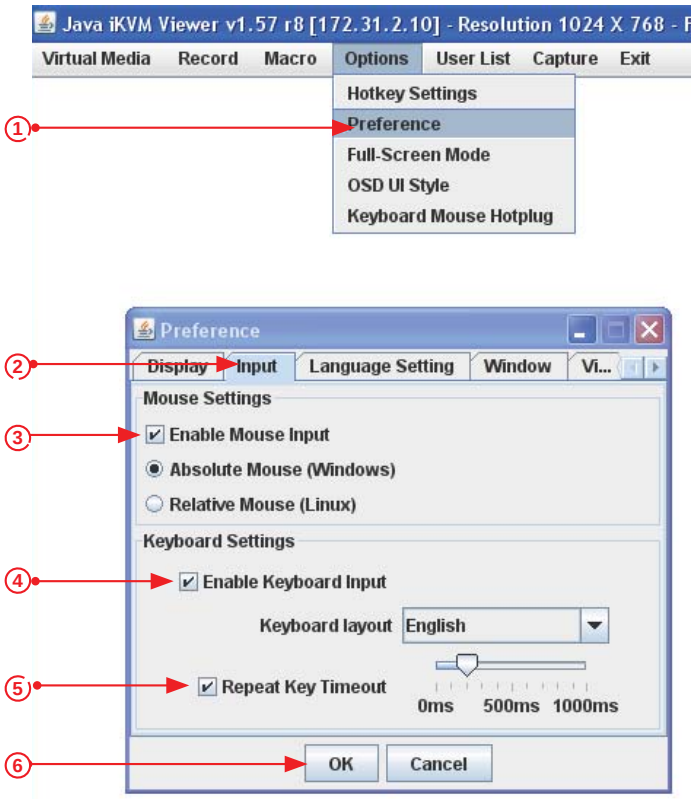
4. Use the slider on the Display Scale to set the appropriate scale setting for your video display from Low (25) to High (100).

5. To ensure the best image quality, select <High Color> for heavier network traffic connections; select <Low Color> for lighter network traffic.

6. Click <OK> to save the recording preference settings or click <Cancel> to cancel the selection.

2.8.1.5.3. Console Redirection - Options: Preference (-Input)

This feature allows you to configure Video_Recording input settings for your console redirection. Click <Input> in the menu bar to activate the Input submenu.



To configure Video Input settings, follow the instructions below.

1. Click <Preference> to invoke the Options submenu.

2. From the Options submenu, click <Input> to invoke the *Input* page to configure mouse and keyboard settings.

3. Check <Enable Mouse Input> to enable mouse support so that you can use the mouse as an input device. Once mouse support is enabled, set a proper mode for your console redirection.

- Select *Absolute_Mode* if you have the Windows OS

- Select *Relative_Mouse* for the Linux OS.

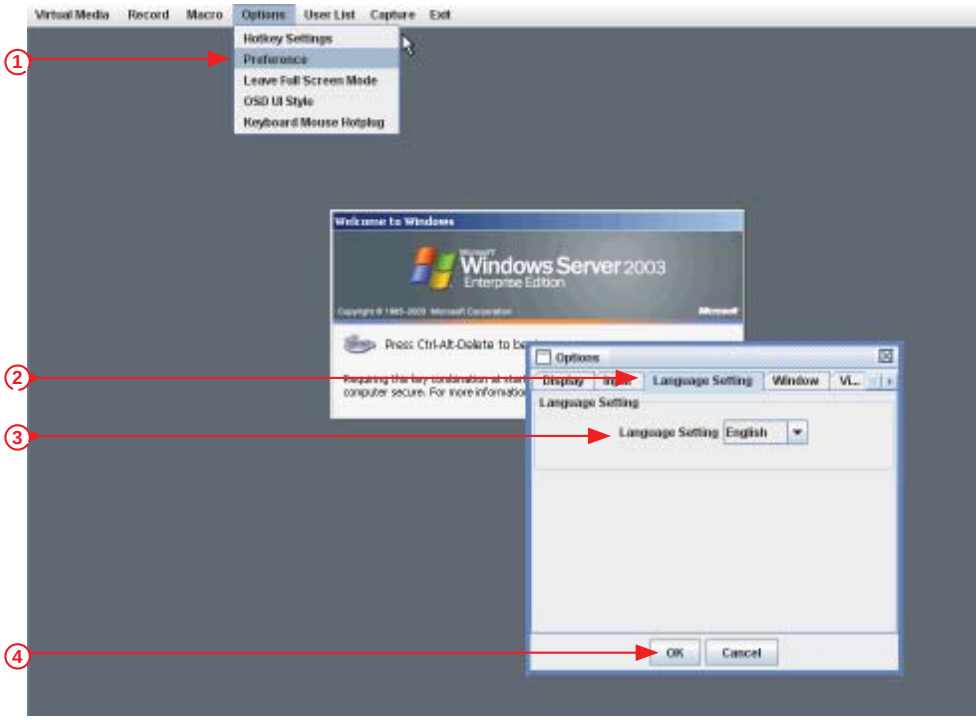
4. Select *Enable Keyboard Input* to enable keyboard support so that you can use soft keyboard as an input device. From the *Keyboard layout* pull-down menu, select the right language setting for your soft keyboard.

5. Use the slider on the *Repeat Key Timeout* scale to select the appropriate timeout settings for repeat keystrokes from 0ms to 1000ms (micro-second).

6. Click <Save> to save the keyboard setting or click <Cancel> to cancel it.

2.8.1.5.4. Console Redirection - Options: Preference (-Language Settings)

This feature allows you to configure Language settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.



To select the correct language setting for your console, follow the steps below.

1. Select *Options* from the Menu bar. From the pull-down menu, select *Preference*.

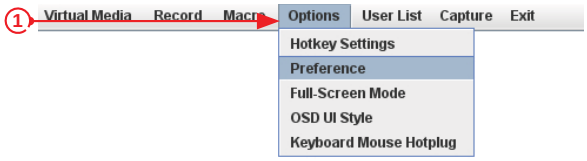
2. Click <Language Setting>.

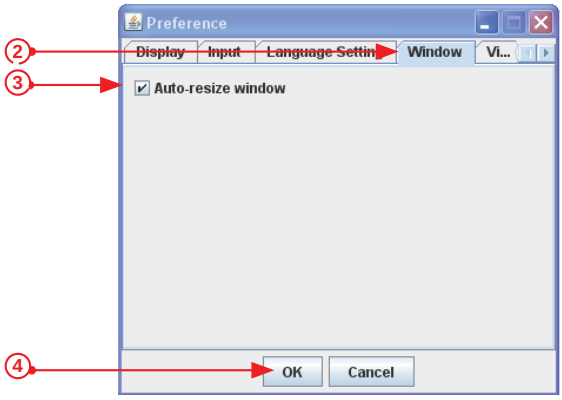
3. From the Language Setting pop-up menu, select the language you want to use for your console redirection. The language options include English, Chinese (Traditional), Japanese, German, French, Spanish, Korean, and Italian.

4. Once you have selected a language setting, click <OK> to use the language.

2.8.1.5.5. Console Redirection - Options: Preference (-Window)

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.





To select the correct Window settings for your console redirection, follow the instructions below.

1. Select *Options* from the Menu bar. From the pull-down menu, select Preference.

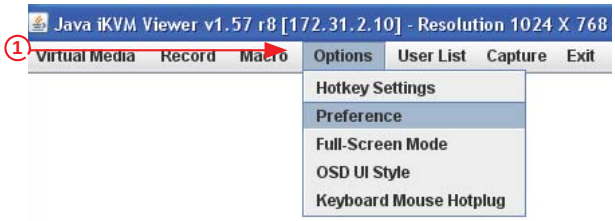
2. Click <Window>.

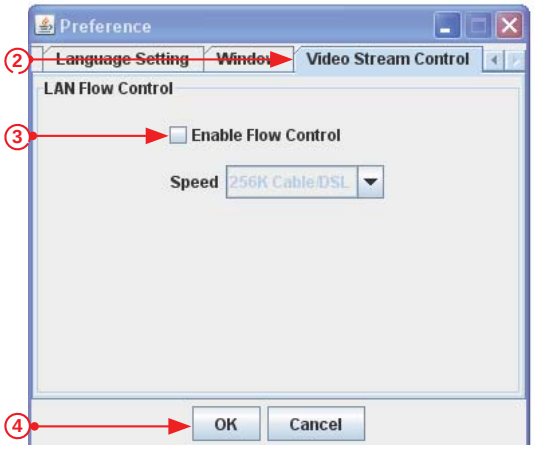
3. Check <Auto Re-size Window> for the system to reset the size of your display window. (If you do not wish your display window to be re-sized automatically, leave the box blank.)

4. Click <OK> to save the window settings.

2.8.1.5.6. Console Redirection - Options: Preference (-Video Stream Control)

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.



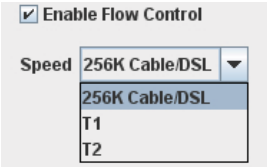


To select the correct Video Stream Control settings for your console redirection, follow the instructions below.

1. Select <Options> from the Menu bar. From the pull-down menu, select *Preference*.

2. Click <Video Stream Control>.

3. Check <Enable Flow Control> to provide support for video flow control. Once the Flow Control support is enabled, select the proper speed for video streaming from the pull-down menu. The speed settings listed below.

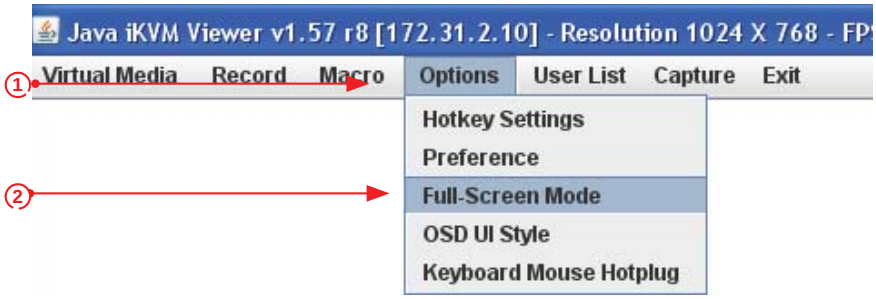


- 256K Cable/DSL
- T1
- T2

4. Click <OK> to save the Video Stream Control setting.

2.8.1.5.7. Console Redirection - Options: Full Screen Mode

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the submenu. From the pull-down menu, select *Full Screen Mode*.

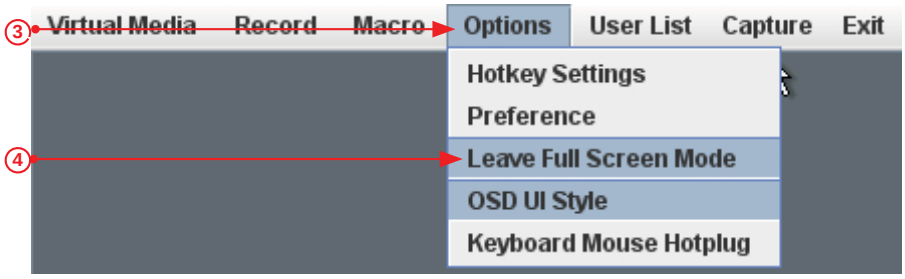


- To Use a Full Screen Display

To set a full_screen display for your console redirection, follow the instructions below.

1. Select <Options> from the menu bar to activate the submenu.

2. Select <Full Screen Mode> from the pull-down menu. Then, press <Enter>. A full-screen display will appear.



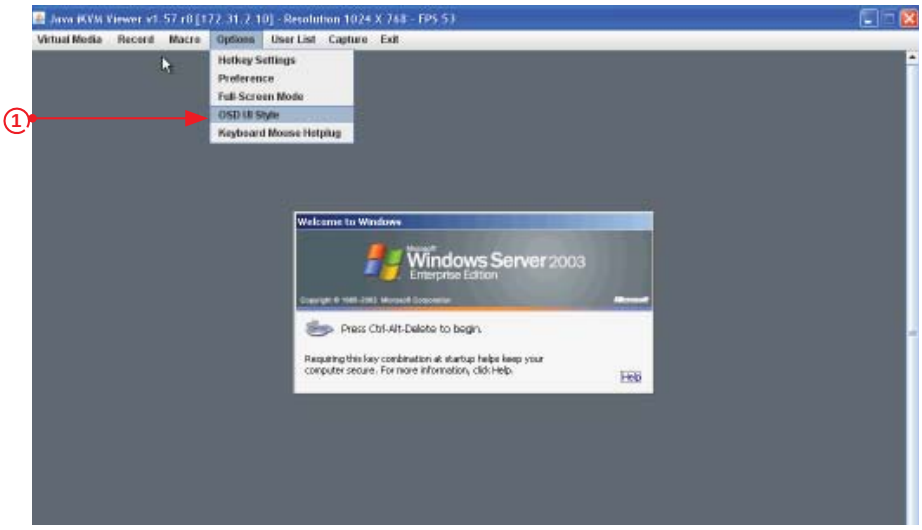
- To Leave the Full_Screen Display

3. To leave the full_screen display, click <Options> to activate its submenu.

4. From the pull-down submenu, select <Leave Full Screen> and press <Enter>.

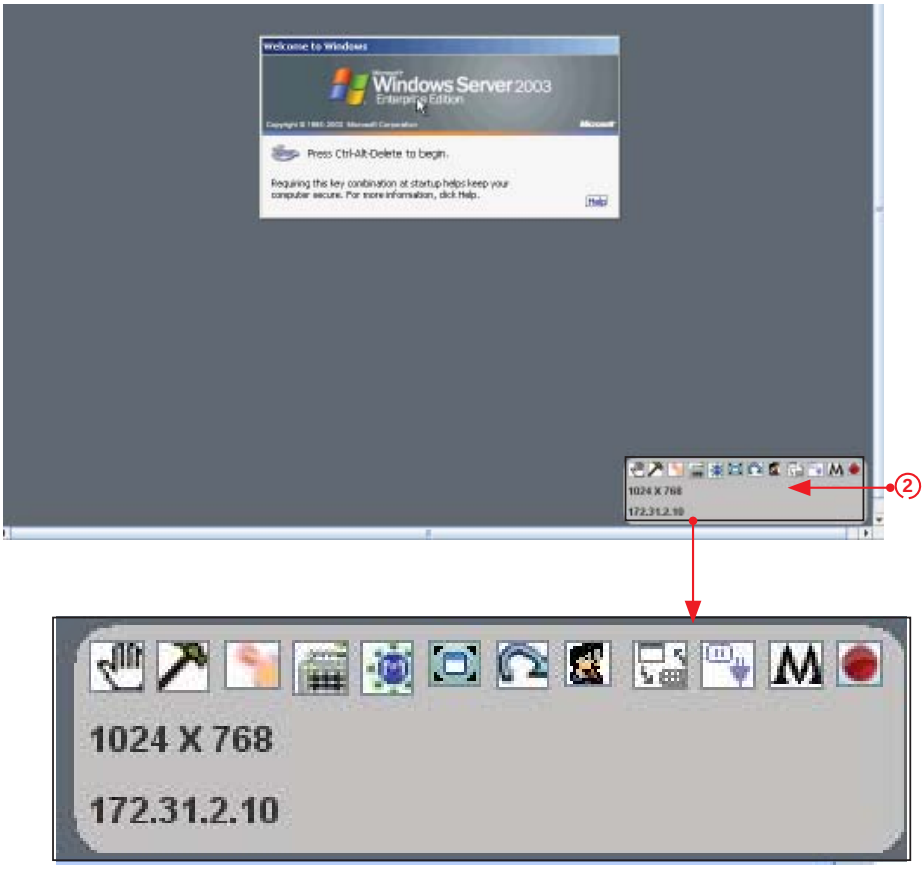
2.8.1.5.8 Console Redirection - Options: OSD UI Style

This feature allows you to configure OSD (On-screen Display) UI (User-Interface) Style settings for your console redirection. To configure the OSD UI settings, follow the steps below.



1. From the Options pull-down menu, click <OSD UI Style> to display the OSD UI Style screen as shown below. This screen provides shortcuts to the main features provided by the firmware for your console redirection.

2. Click an <OSD_UI_Style> icon to change the settings listed on the next page.



The OSD UI Style Screen Close-up

The OSD UI Style Screen Close-up

1. **Move OSD UI Screen:** Click this icon to move the OSD_UI Screen to a new location on the display.

2. **Hotkey Settings:** Click this icon to access the Hotkeys submenu and change the settings.

3. **Virtual Media:** Click this item to access the Virtual Media submenu and configure the settings.

4. **Virtual Keyboard:** Click this item to access the Virtual Keyboard submenu and use your virtual (soft) keyboard.

5. **Preferences submenu:** Click this item to access the References submenu as indicated in the previous sections.

6. **Full Screen Mode:** Click this item to change the size of your display window to the full screen mode.

7. **Exit Remote Console:** Click this item to exit from the remote connection.

8. **Users List:** Click this item to display the user list.

9. **Change Tool Bar Display:** Click this item to change the tool_bar display format.

10. **Hotplug Keyboard/Mouse:** Click this item to hotplug keyboard and mouse.

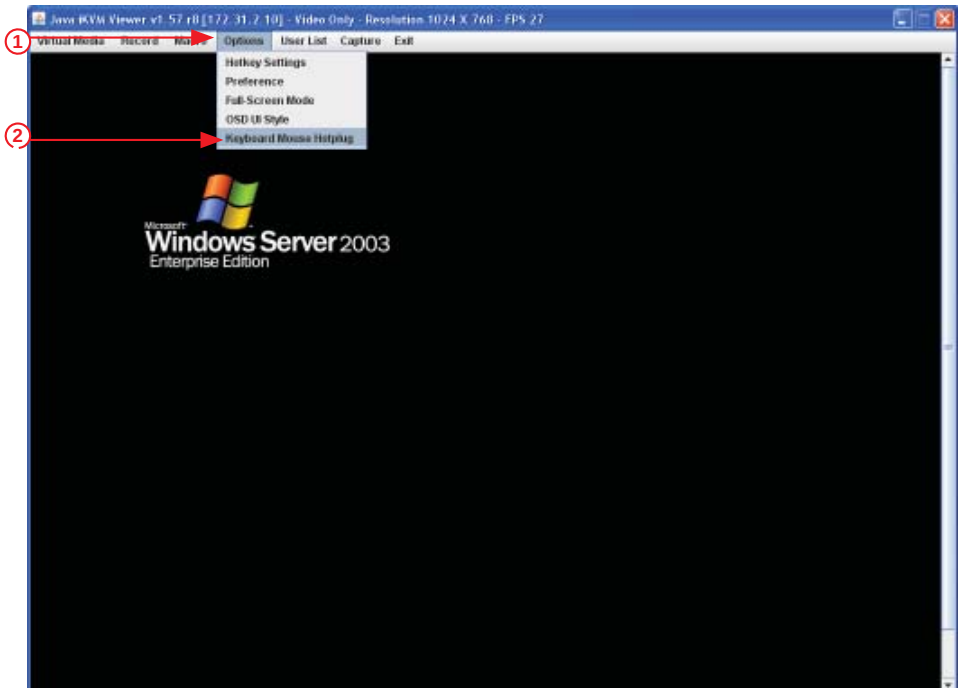
11. **Macro:** Click this item to enable Macro support and use Macro features.

12. **Video Recording:** Click this item to access the Video Recording submenu and to use video recording.

13. **Image Size:** This item displays the image size in pixel.

14. **IP Address:** This item displays the IP Address of IPMI.

2.8.1.5.9 Console Redirection - Keyboard/Mouse Hotplug

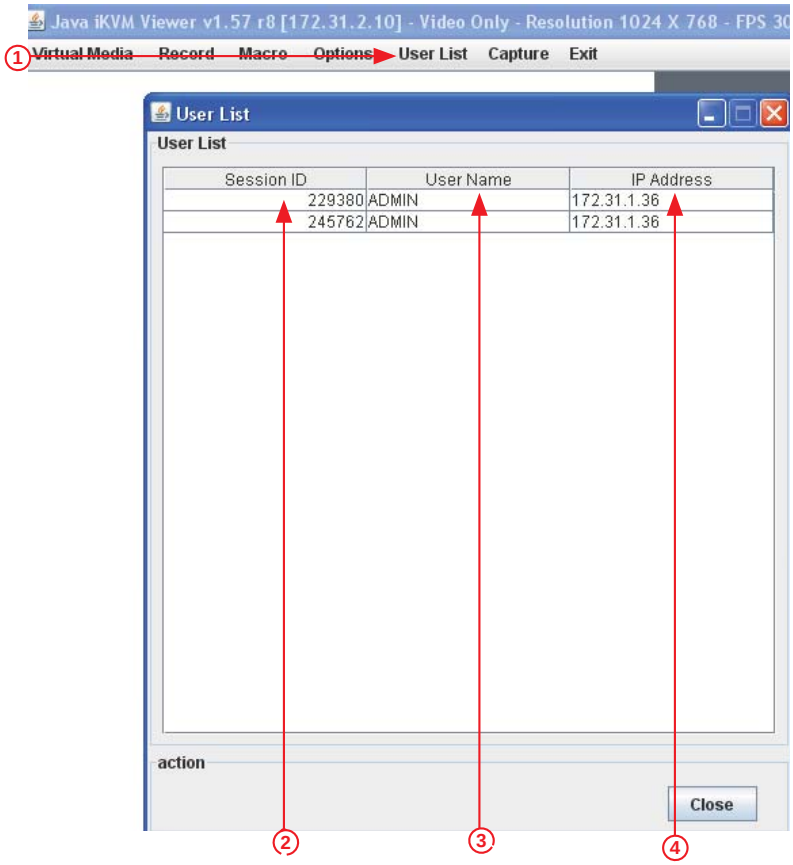


1. Click <Options> on the menu bar to invoke the pull-down submenu.

2. Click <Keyboard/Mouse Hotplug> from the pull-down menu to enable keyboard/mouse hotplug support for your console redirection.

2.8.1.6 Console Redirection - User List

This feature allows you to access the user list. To configure User List settings, follow the instructions below.



1. From the menu bar, click <User List> to display the User List screen as shown above.

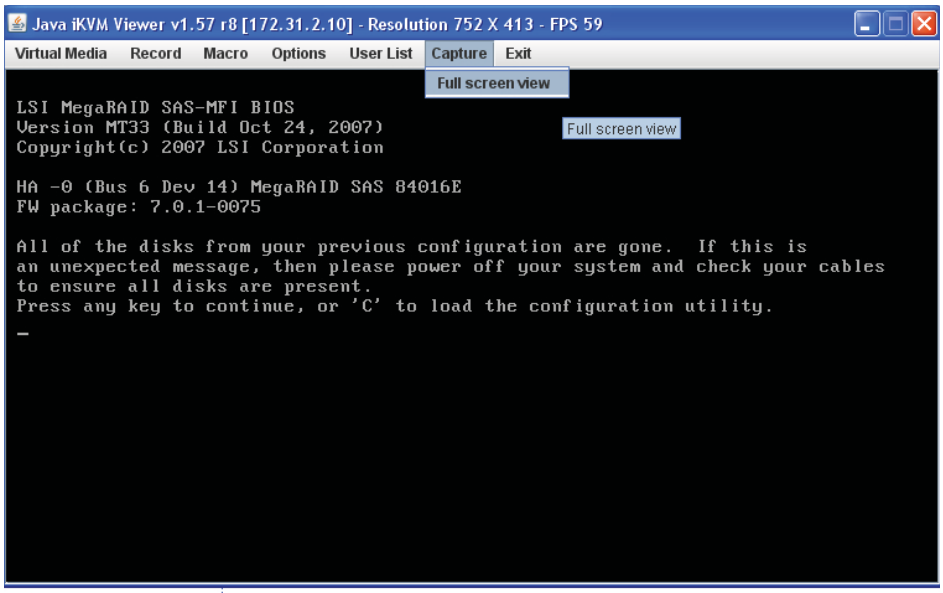
2. **Session ID:** This item displays the current session ID#.

3. **User Name:** This item displays the name(s) of the user(s).

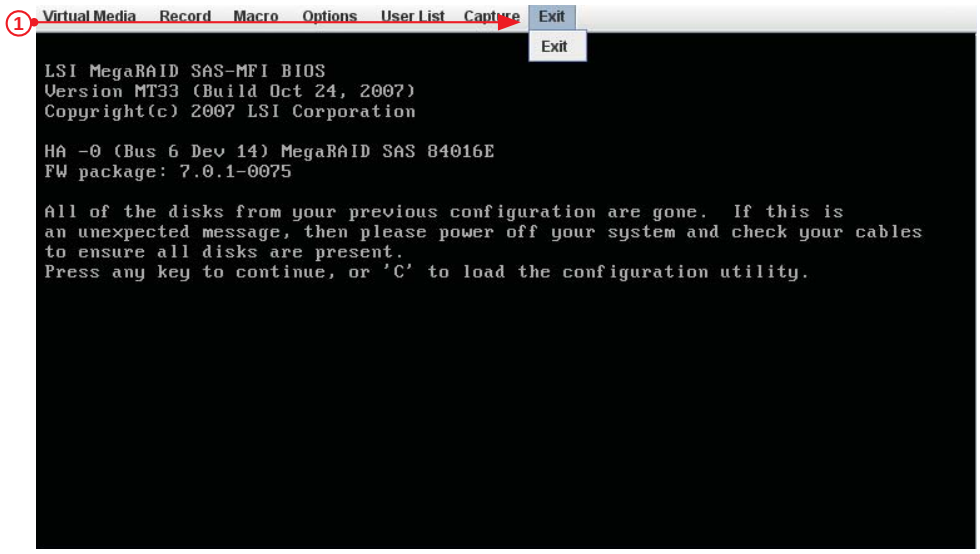
4. **IP Address:** This item displays the IP Address of the client server.

2.8.1.7 Console Redirection - Capture

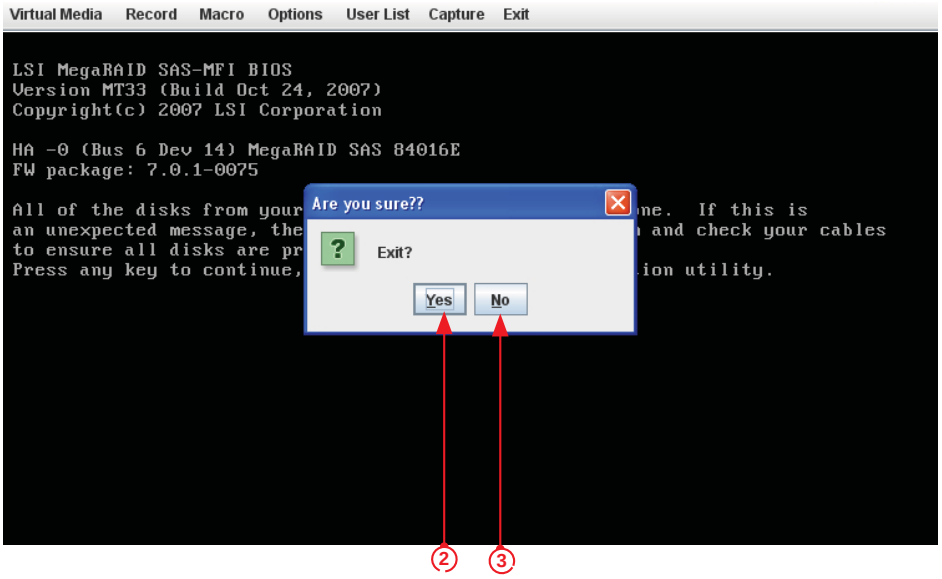
This feature allows you to capture the screen displayed on your remote console.


Java iKVM Viewer v1.57 r8 [172.31.2.10] - Resolution 752 X 413 - FPS 59
Virtual Media
Record
Macro
Options
User List
Capture
Exit
Full screen view
Full screen view
LSI MegaRAID SAS-MFI BIOS
Version MT33 (Build Oct 24, 2007)
Copyright(c) 2007 LSI Corporation
HA -0 (Bus 6 Dev 14) MegaRAID SAS 84016E
FW package: 7.0.1-0075
All of the disks from your previous configuration are gone. If this is
an unexpected message, then please power off your system and check your cables
to ensure all disks are present.
Press any key to continue, or 'C' to load the configuration utility.

2.8.1.8 Console Redirection - Exit


Virtual Media
Record
Macro
Options
User List
Capture
Exit
Exit
LSI MegaRAID SAS-MFI BIOS
Version MT33 (Build Oct 24, 2007)
Copyright(c) 2007 LSI Corporation
HA -0 (Bus 6 Dev 14) MegaRAID SAS 84016E
FW package: 7.0.1-0075
All of the disks from your previous configuration are gone. If this is
an unexpected message, then please power off your system and check your cables
to ensure all disks are present.
Press any key to continue, or 'C' to load the configuration utility.
1

1. To exit from Console Redirection, click <Exit>.

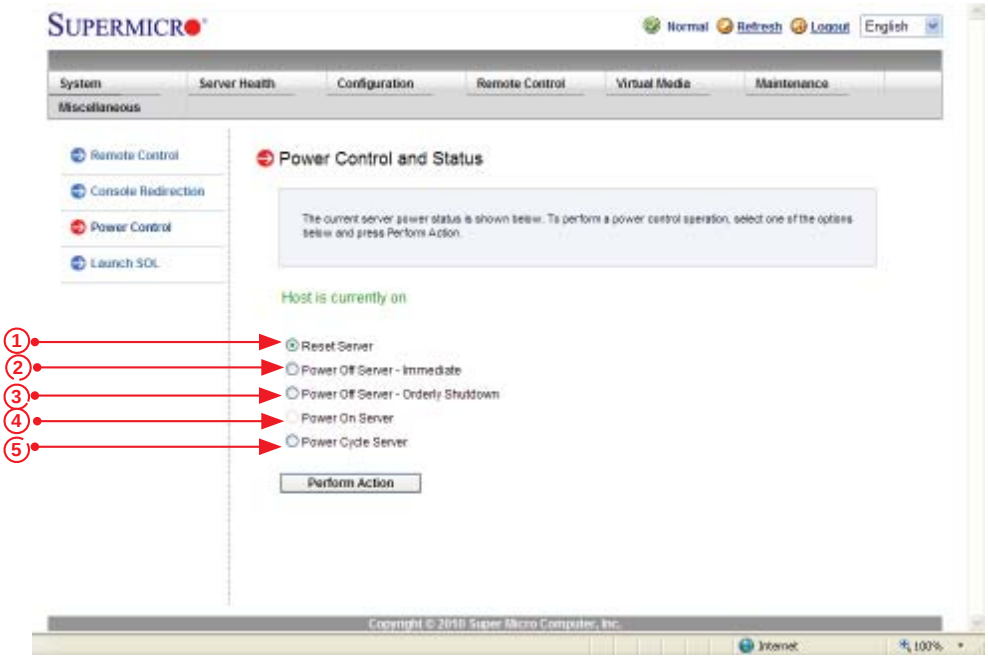


2. At the prompt- "Are you sure?", click <Yes> to exit from remote redirection.

3. Click <No> to return to the current session.

2.8.2 Remote Control - Server Power Control

This feature allows the user to check power state and perform remote power control.



1. Click <Reset Server> and press <Perform Action> to reset the host server.

2. Click <Power Off Server - Immediately> and press <Perform Action> to power off the remote server immediately.

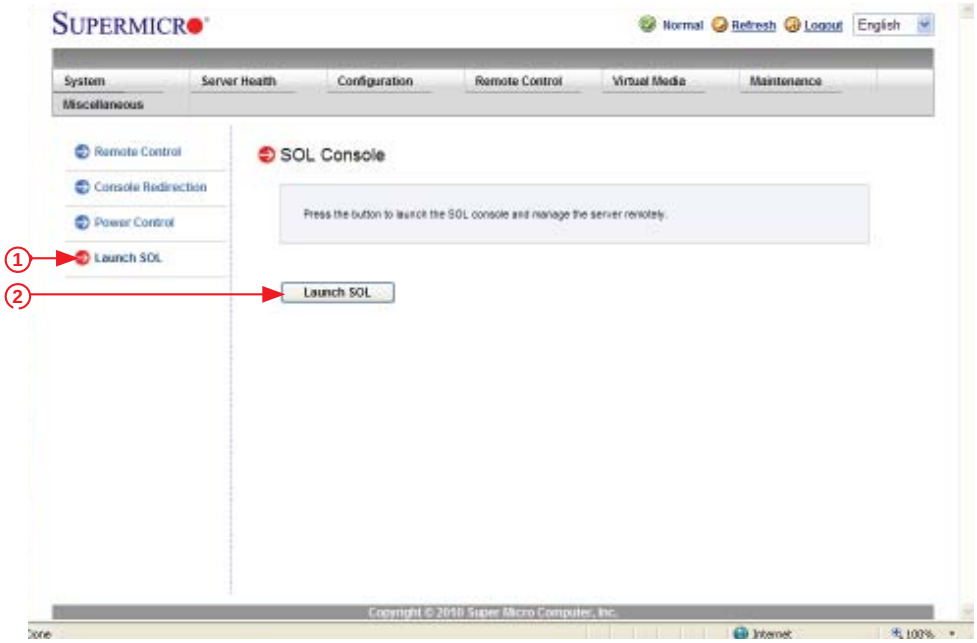
3. Click <Power Off Server - Orderly Shutdown> and press <Perform Action> to power off and shutdown the remote server orderly.

4. Click <Power On Server> and press <Perform Action> to power on the remote server.

5. Click <Power - Cycle Server> and press <Perform Action> to reset the power cycle of the remote server.

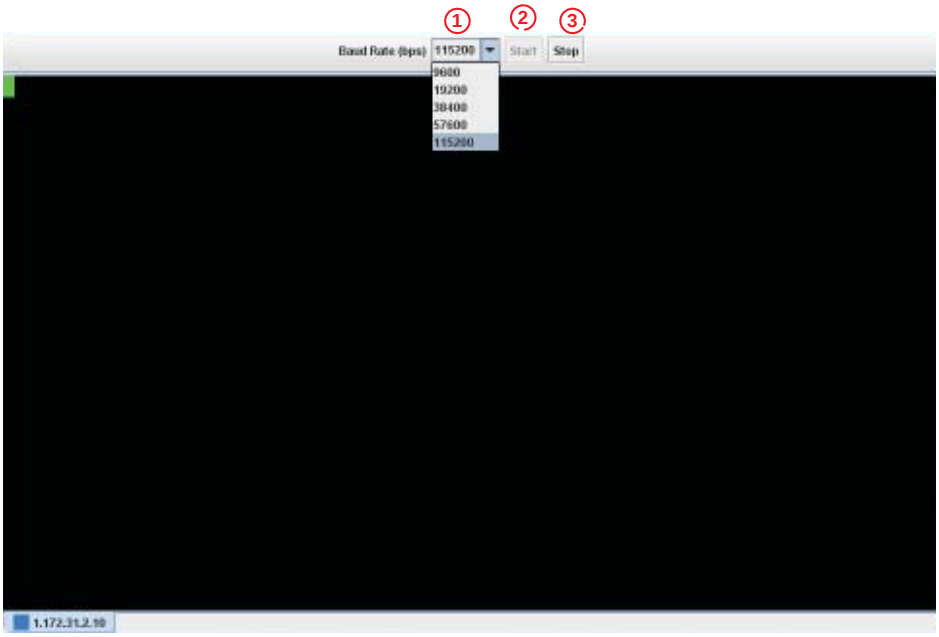
2.8.3 Remote Control-Launch SOL

This feature allows you to launch the remote console by using SOL (Serial_over_LAN). This feature provides serial port connections over LAN to allow the user to access a host server via Console Redirection. It also allows a system administrator to monitor and manage a server from a remote site. To launch SOL, follow the instructions below.



1. Click <Launch SOL> in the left Options window to enable SOL (Serial Over LAN) support.

2. Click the <Launch SOL> button to launch SOL. After SOL is launched, the following screen will display as shown on the next page.



Launching SOL

1. You can select a Baud Rate (bps) from the pull-down menu as your SOL transfer rate. The options are listed below. Make sure that the Baud Rate selected here matches the Baud Rate set in the BIOS.

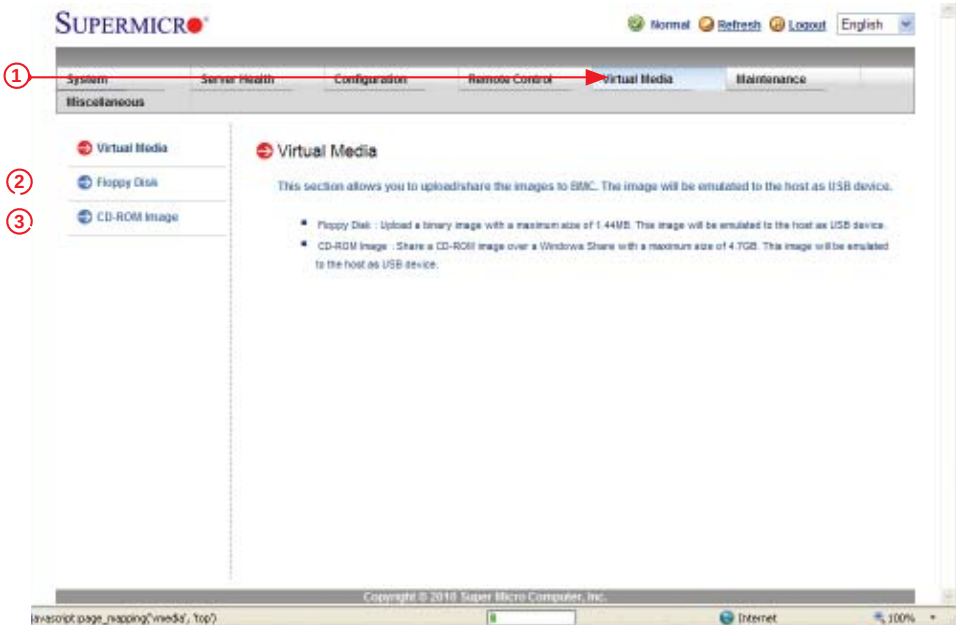
- 9600 bps (bit-per-second)
- 19200 bps
- 38400 bps
- 57600 bps
- 115200 bps
- Manufacture Default.

2. Once you've selected the Baud rate, press <Start> to start the session.

3. You can also press <Stop> to stop SOL connection.

2.9 Virtual Media

This feature allows you to upload and share images via the BMC (Baseboard Management Controller). These images will be emulated to the host server as USB applications. To follow the Virtual Media settings, follow the instructions below.


SUPERMICRO
Normal
Refresh
Logout
English
System
Server Health
Configuration
Remote Control
Virtual Media
Maintenance
Miscellaneous
1
Virtual Media
2
Floppy Disk
3
CD-ROM Image
Virtual Media
This section allows you to upload/share the images to BMC. The image will be emulated to the host as USB device.
Floppy Disk : Upload a binary image with a maximum size of 1.44MB. This image will be emulated to the host as USB device.
CD-ROM Image : Share a CD-ROM image over a Windows Share with a maximum size of 4.7GB. This image will be emulated to the host as USB device.
Copyright © 2018 Super Micro Computer, Inc.
Internet
100%

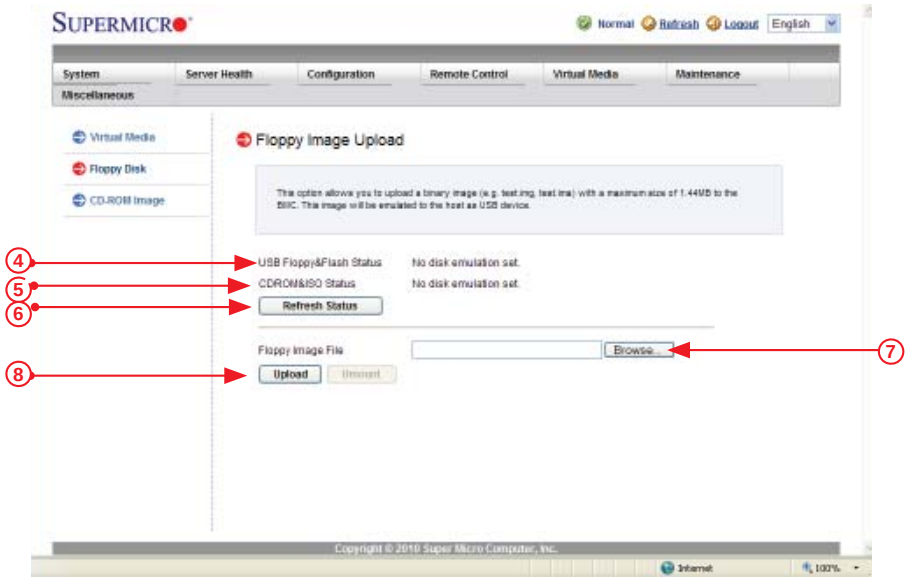
1. Click <Virtual Media> to configure virtual media settings for your remote console, including Floppy Disk and CD-ROM image settings.

2. Click <Floppy Disk> on the Options Window to configure the floppy disk settings for your console redirection. The Floppy Disk screen will display as shown on the next page.

3. Click <CD-ROM Image> to configure CD-ROM image settings for your console redirection. When you click on this item, the screen on Page 2-55 displays.

2.9.1 Configuring USB Floppy & Flash Device Settings

To configure CD ROM image files for sharing, follow the instructions below.



4. *USB Floppy & Flash Status* displays the status of a USB floppy or a flash device.

5. *CDROM & ISO Status* displays the status of a CDROM or an ISO device.

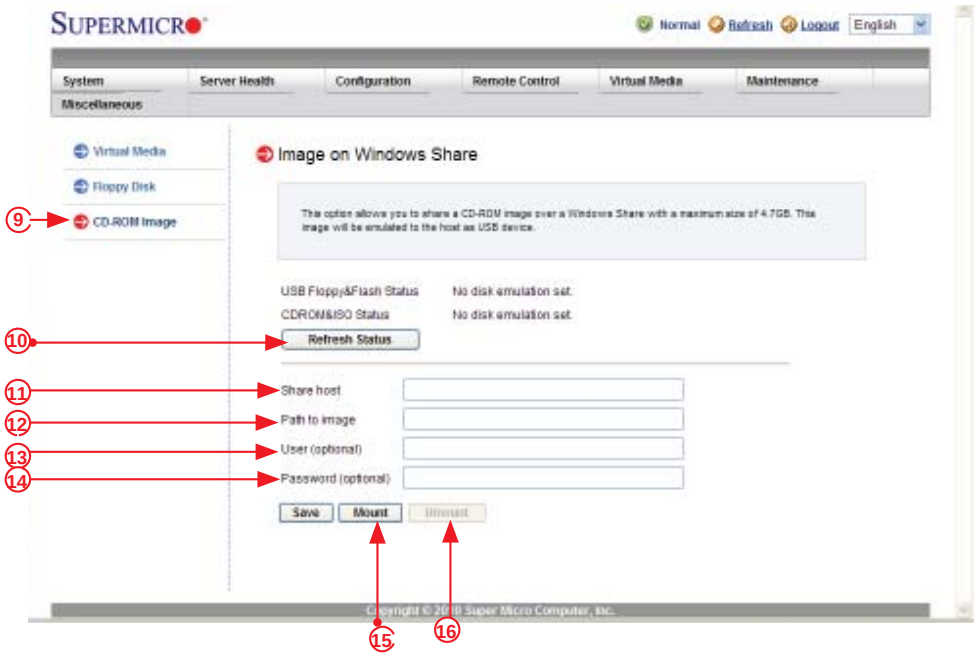
6. Click <Refresh Status> to refresh the USB floppy or the flash device.

7. Click <Browse> to select an image file from your data base for your console redirection.

8. After you've selected your image file, click <Upload> to upload your image file to the server.

2.9.2 Configuring CD ROM Image File Settings

To configure CD ROM image files for sharing, follow the instructions below.



9. Click <CD-ROM Image File> to invoke the <Image on Windows Share> screen as shown above. The following items will display.

- *USB Floppy & Flash Status* indicates the status of a USB floppy or a flash device.

- *CD ROM & ISO Status* indicates the status of a CD-ROM or an ISO device.

10. Click <Refresh Status> to refresh *USB Floppy/Flash* and *CD ROM/ISO* devices.

11. Enter the *Share_Host* server for your console redirection.

12. In the *Path_to_Image* field, enter the path to the CD-ROM image file for sharing.

13. In the *Users (Optional)* field, specify the users that have access to the CD-ROM image files. (This item is optional).

14. In the *Password (Optional)* field, enter your user password. (Optional.)

15. To *mount* an image file, follow the steps below.

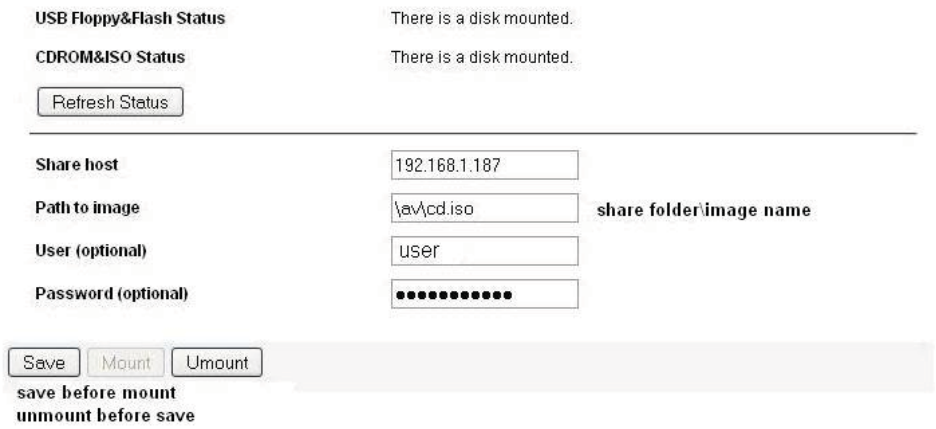
    1. Click <Save>.

    2. Click <Mount>.

3. To *unmount* an image file, follow the steps below.

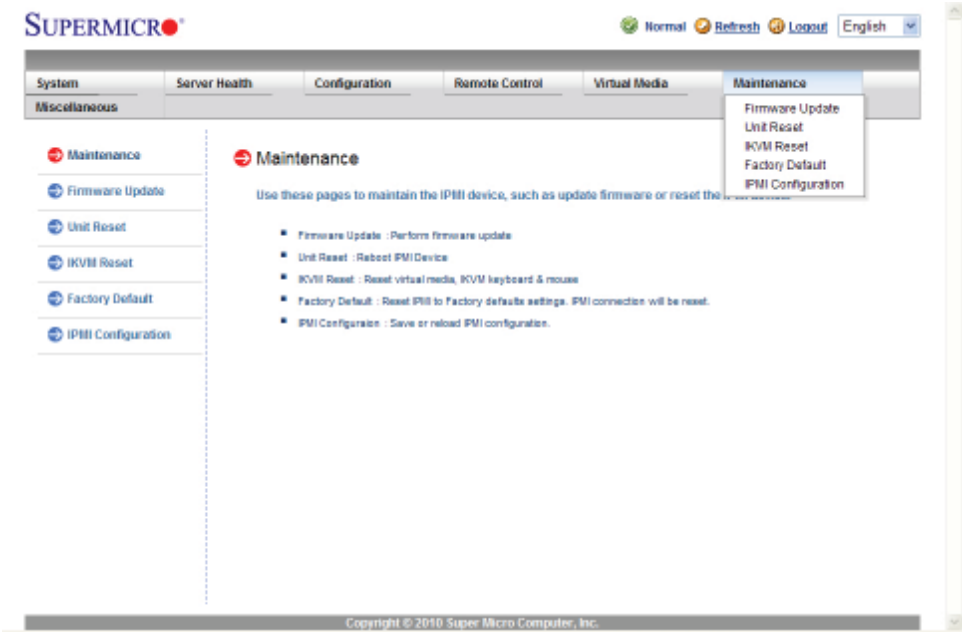
   1. Click <Unmount>.

   2. Click <Save>.



2.10 Maintenance

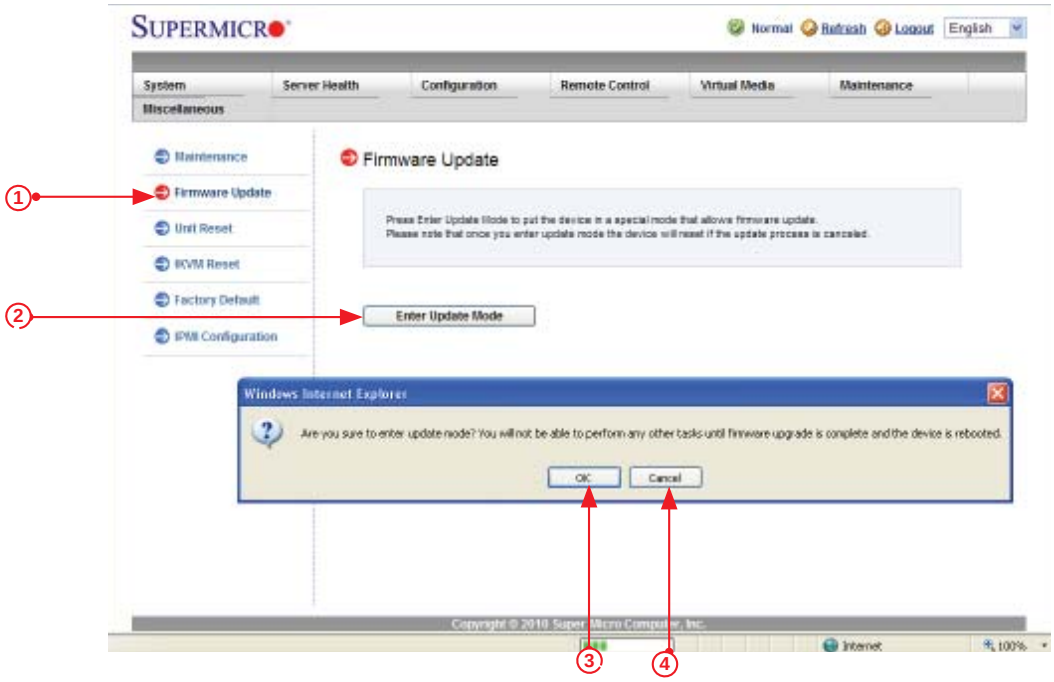
Use this feature to manage and configure IPMI device settings.



Click the <Maintenance> icon in the menu bar to invoke the *Maintenance* main screen as shown above. The *Maintenance* menu includes the following items.

- **Firmware Update:** Click this item to update the remote server's BMC firmware. The Firmware Update screen is shown in the next section.
- **Unit Reset**: Click this item to reboot the BMC (IPMI) controller.
- **IKVM Reset**: Click this item to reset the IKVM setting.
- **Factory Default**: Click this item to restore IPMI to the factory default settings.
- **IPMI Configuration**: Click this item to save IPMI configuration settings to a file or to load IPMI configuration settings from a file.

2.10.1 Maintenance - Firmware Update



Firmware Update

To update IPMI Firmware, follow the instructions below.

1. Click <Firmware Update> in the Options Window.

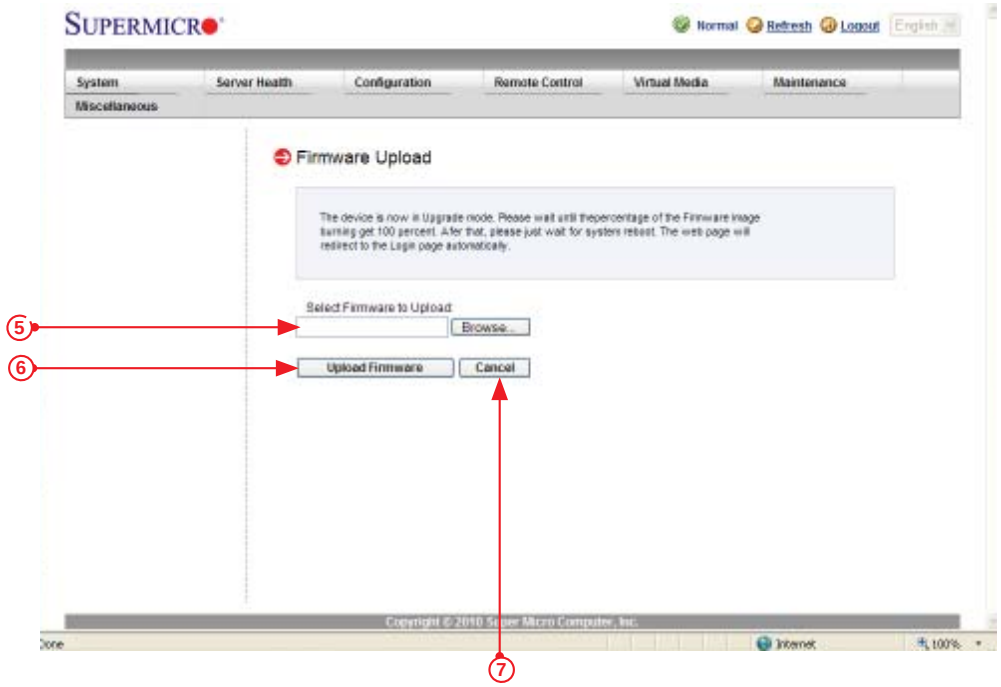
2. Click <Enter Update Mode> to enter the update mode. A warning message will display.

   Warning: Once the server is in the firmware update mode, the device will be reset, and the server will reboot even if you cancel firmware updating.

3. Click <OK> to update your IPMI firmware. Once you've clicked OK to update the firmware, the *Firmware Upload* screen will display as shown on the next page.

4. Click <Cancel> to cancel firmware updates.

Once you have clicked <OK> to update the IPMI Firmware, the following Firmware Upload screen will display as shown below.



5. Enter the name of the firmware you wish to upload. You can also select a firmware from the pull-down menu to upload.

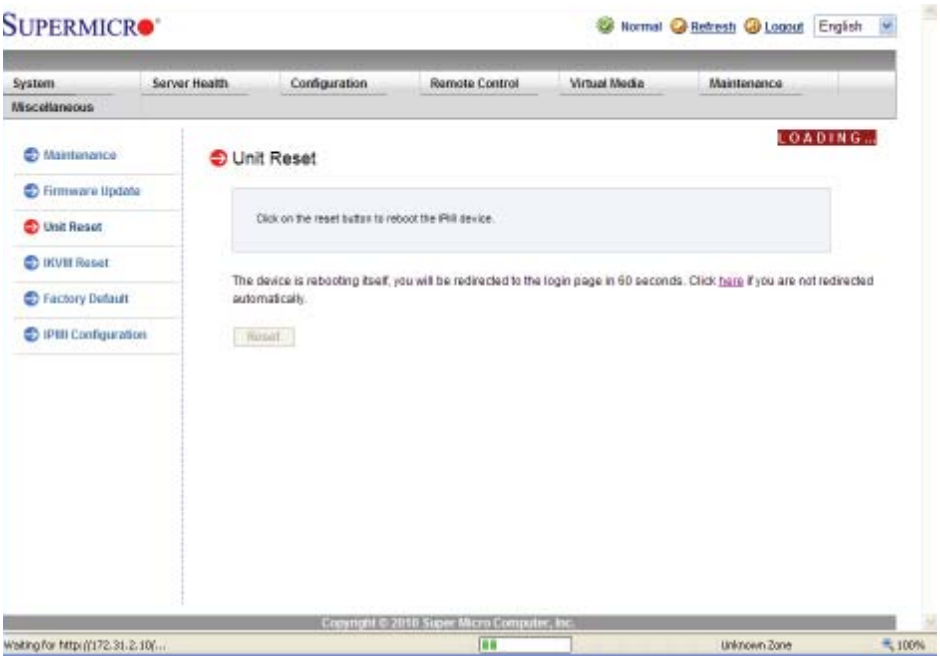
6. Click <Upload Firmware> to upload the selected firmware to the host server.

   Warning! To properly update your firmware, do not interrupt the process until the process is completed. Once it is completed, the system will automatically reboot, and you will need to login to the server again.

7. Click <Cancel> to abort firmware uploading.

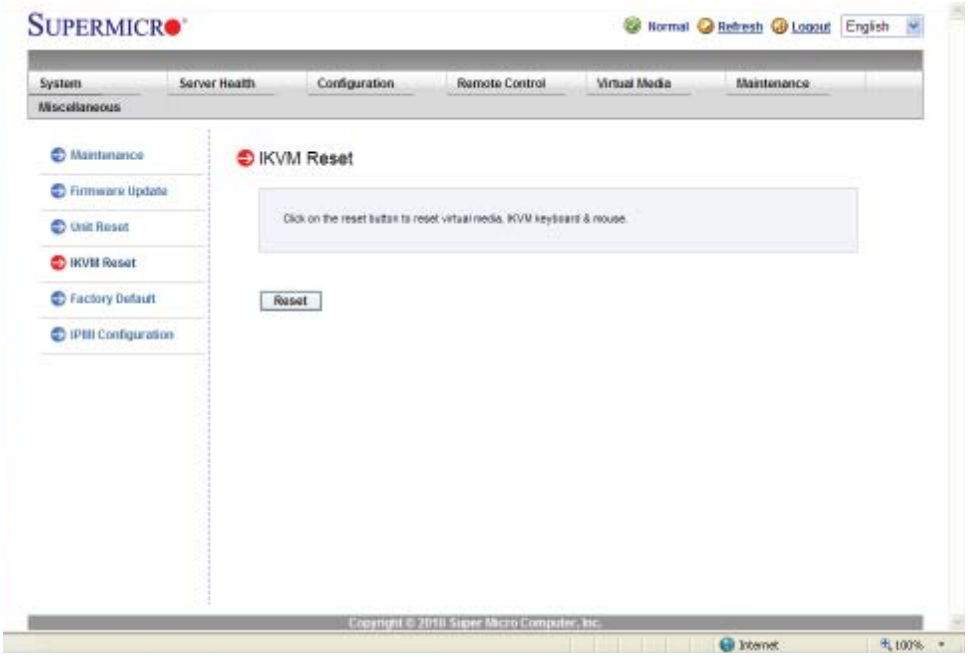
2.10.2 Maintenance - Unit Reset

Use this feature to reset the IPMI device.



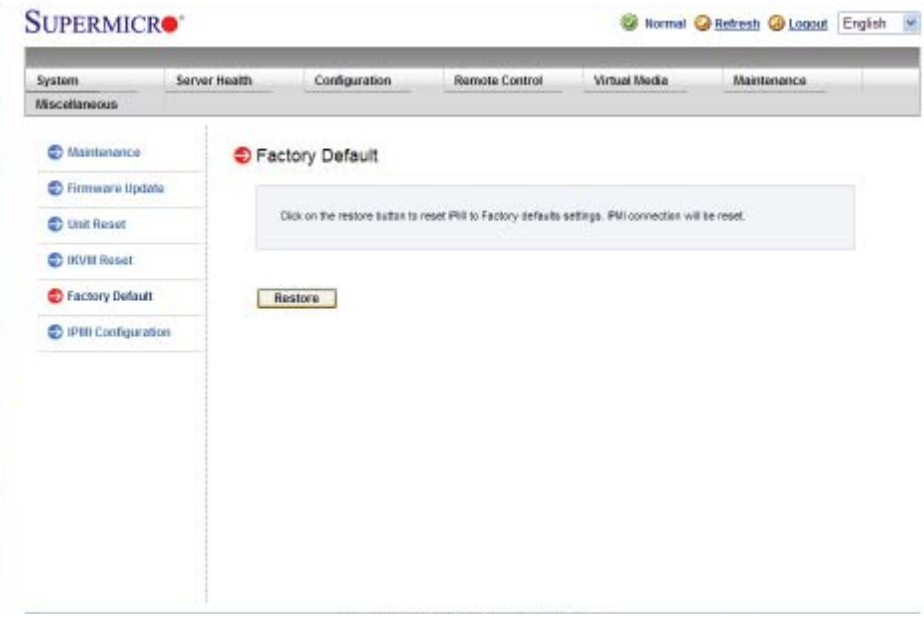
2.10.3 Maintenance - IKVM Reset

This feature allows you to reset IKVM. It will reset virtual media, IKVM keyboard and mouse.



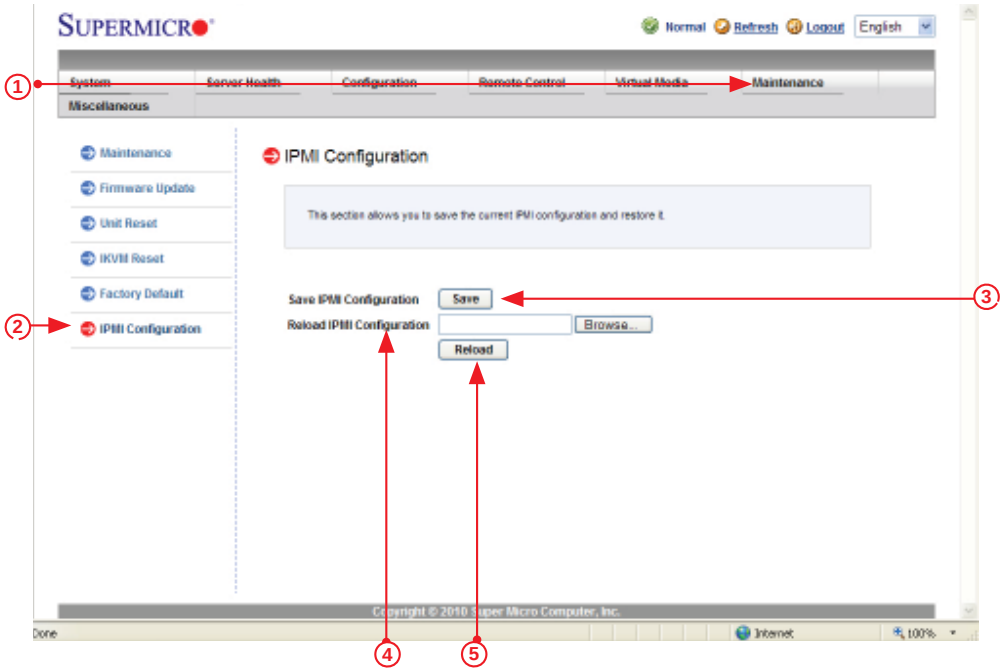
2.10.4 Maintenance - Factory Default

This feature allows the user to restore IPMI to factory default settings.



2.10.5 Maintenance - IPMI Configuration

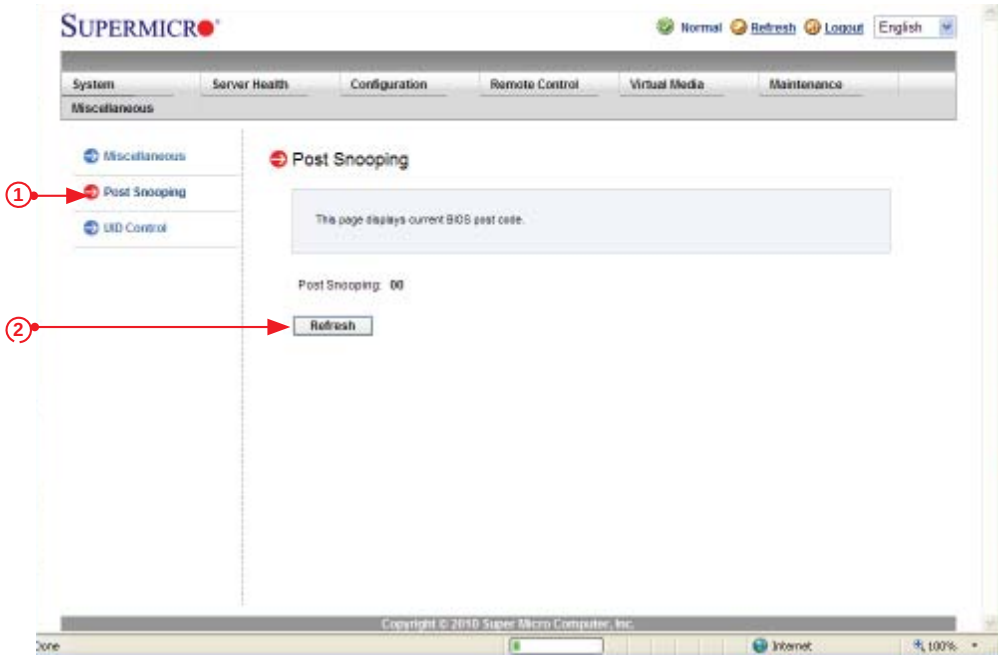
This feature allows the user to save IPMI configuration settings. To save the IPMI configuration settings, follow the instructions below.



- To save the IPMI Configuration settings, click <Save> and enter a file name.
- To load IPMI Configuration settings from a previously saved file, click <browse> and select a file. Then, click <reload>.

2.11 Miscellaneous

This feature allows the user to perform various network activities including POST (Power-On-Self Test) code query and turning-on/-off UID control. To query POST codes or to turn on/off UID control, follow the instructions below.



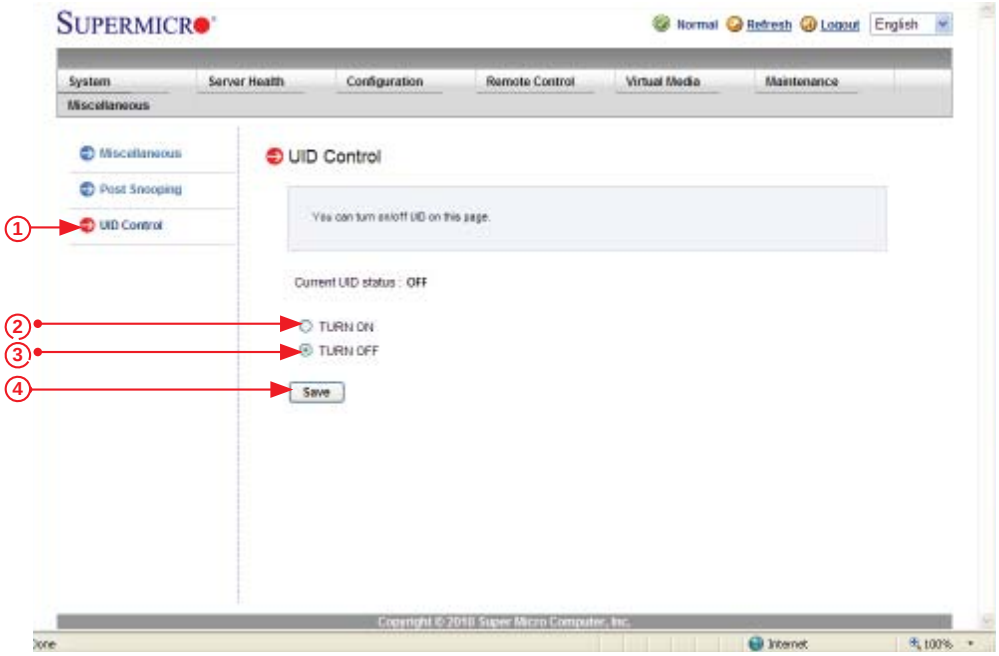
2.11.1 Miscellaneous - POST Snooping

1. Click <Post Snooping> in the Options window. The *Post Snooping* screen will display as shown above.

2. Click <Refresh> to query the POST Snooping code for BIOS LPC Port80.

2.11.2 Miscellaneous - UID Control

This feature allows the user to turn-on or turn-off UID (Unit Identification) control. To turn on or off UID control, follow the instructions below.



1. Click <UID Control> in the *Options* window. The <UID Control> screen will display as shown above. It will also show the current UID Control status.

2. Click <Turn On> to turn on UID control.

3. Click <Turn Off> to turn off UID control.

4. Click <Save> to save the setting.

Notes

Chapter 3

Frequently Asked Questions

3-1 Frequently Asked Questions

A. Question: How do I flash the IPMI firmware?

Answer:

Method#1

1. Click the <Maintenance> button. Browse the files available and select the correct file to flash the firmware.

2. Click the <Update Firmware> button to proceed with firmware flashing.

Method#2

- You can flash the IPMI firmware using flash tools located at

ftp://ftp.supermicro.com/utility/IPMI FW flash tools/.

- For the latest IPMI Firmware, please refer to

ftp://ftp.supermicro.com/firmware/nuvoton/.

B. Question: If I am using a firewall for my network connections, which ports should I open so that I can access my IPMI connection?

Answer: In order to access your IPMI connection behind a firewall, please open the following ports:

HTTP: 80 (TCP)

HTTPS: 443 (TCP)

IPMI: 623 (UDP)

Remote console: 5900 (TCP)

Virtual media: 623 (TCP)

SMASH: 22 (TCP)

WS-MAN: 8889 (TCP)

C. Question: When I update IPMI firmware through web, I got a file download pop-up, but the firmware was not updated. Why?

Answer: This may be caused by your anti-virus software. Some anti-virus software can cause this. Disable your anti-virus software temporarily and update your firmware.

D. Question: My system seems to function properly; however, the IPMI event log indicates that my voltage and temperatures are beyond the limits. Why?

Answer: It is not a normal condition. Make sure that there is no other device accessing the I^2C bus. If another device accesses the I^2C bus frequently, it might cause a collision with the BMC when this device accesses the I^2C bus. When you see this error, please uninstall lm_sensors in the Linux.

Appendix A

Flash Tools

A-1 Overview

This chapter provides instructions on how to use Aten Flash Tools. Aten Flash Tools Utility supports firmware updates and firmware dumping.

1. Firmware Updates

The Aten Flash Tools utility provides a complete solution for firmware updates. The user can flash the firmware using DOS, Windows or Linux. In addition, Windows and Linux allow the user to update the firmware via LAN or KCS.

2. Firmware Dumping

In addition to firmware updating, Aten Flash Tools also support firmware_dumping from the BMC (Baseboard Management Controller). You can use this feature to back up the firmware by *dumping* the current version of the firmware to an archive folder before updating to a new version. It will also allow you to flash other BMCs in the factory for mass production. Firmware_dumping is supported by DOS, Windows and Linux.

A-2 Reference

Aten Flash Tools Utility was built in reference to the IPMI - Intelligent Platform Management Interface Specification Second Generation v2.0, Document Revision 1.0, February 12, 2004, by Intel, Hewlett-Packard, NEC, and Dell.

A-3 Using Aten Flash Tools in the DOS Environment

To use the Aten Flash Tools in DOS, follow the steps below:

1. Enter <dupdate.exe> and press <Enter>.

2. The information about the utility will be displayed. Follow the instructions given on the screen to configure the settings as shown in Figure 1.

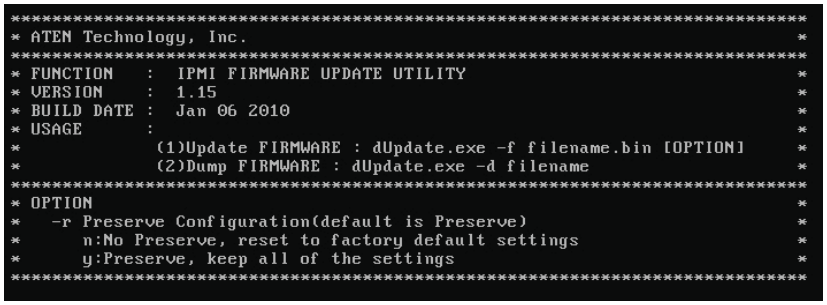

* ATEN Technology, Inc.
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY
* VERSION : 1.15
* BUILD DATE : Jan 06 2010
* USAGE :
(1)Update FIRMWARE : dUpdate.exe -f filename.bin [OPTION]
(2)Dump FIRMWARE : dUpdate.exe -d filename
* OPTION
-r Preserve Configuration(default is Preserve)
n:No Preserve, reset to factory default settings
y:Preserve, keep all of the settings

Figure 1: IPMI Firmware Updates Utility in DOS - Main Screen

The main screen of the IPMI Update Utility for DOS (above) displays the version and the built date of the utility currently used in the system. The DOS version of Flash Tools Utility allows the user to update or dump the firmware via KCS channels.

Firmware Updating via KCS Channels

To update your firmware via KCS, type <dUpdate.exe –f [filename.bin] *–r y*.> After entering this command, a screen will display as shown in Figure 2.

1. –f: Type <-f> to enter the file name of the firmware that you want to update.

2. –r: Type <-r> to preserve the configuration settings you've chosen. This feature is optional. The default setting is to "preserve" the configuration.

3. y: Type <y> for the BMC to keep all settings after the firmware is updated; otherwise, the BMC will reset all settings to factory default.

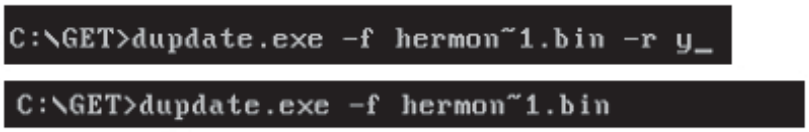


Figure 2: Examples of Firmware Updates with or without the "Preserved" Command

After you've entered the commands above, Aten Flash Tools will start to update the firmware. There are two phases in firmware updating.

1. Phase 1 is to transfer the FW image file to the BMC. In this phase, Flash Tools will transfer three parts to the BMC as shown in Figure 3, Figure 4 and Figure 5.

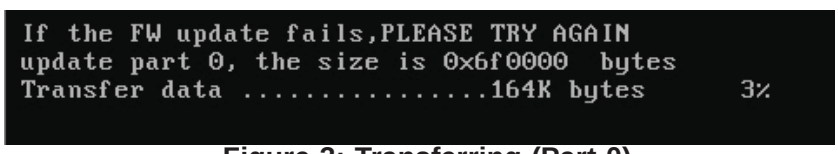


Figure 3: Transferring (Part 0)

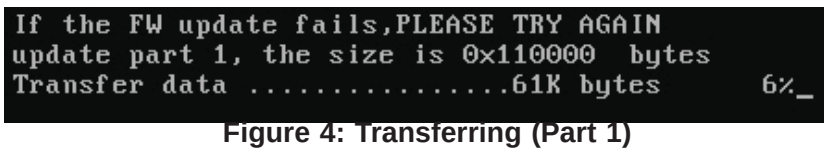


Figure 4: Transferring (Part 1)

Figure 5: Transferring (Part 2)

2. Phase 2 is to flash the new firmware. The progress of firmware updating will be displayed as shown in Figure 6. The BMC will reboot after the firmware is completely updated. Please wait for the BMC to complete system reboot (Figure 7).

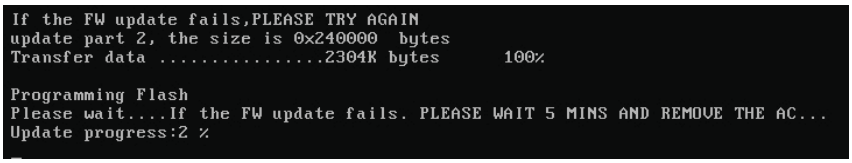

If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....2304K bytes 100%
Programming Flash
Please wait....If the FW update fails. PLEASE WAIT 5 MINS AND REMOVE THE AC...
Update progress:2 %

Figure 6: Progress of Firmware Updating

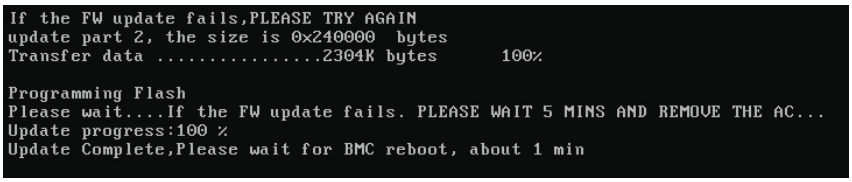

If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....2304K bytes 100%
Programming Flash
Please wait....If the FW update fails. PLEASE WAIT 5 MINS AND REMOVE THE AC...
Update progress:100 %
Update Complete,Please wait for BMC reboot, about 1 min

Figure 7: Updates Completed

Dumping Firmware from the BMC via KCS channels

The user can dump the firmware by typing <dupdate.exe –d [filename].> Flash Tools will dump the firmware into the file that the user has assigned in the previous command. In the example given in Figure 8, Flash Tools will dump the firmware to dump_img.

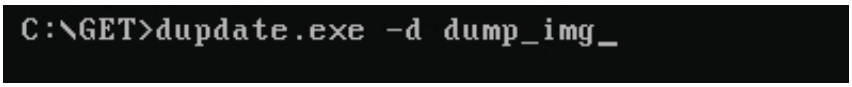


Figure 8: Example of Firmware Dumping via KCS

There are two phases in firmware dumping.

1. During Phase 1, the Flash Tools Utility is waiting for the BMC to prepare the firmware for dumping. As soon as preparation is complete, the Flash Tools Utility will enter Phase 2.

2. In Phase 2, the Flash Tools utility gets the firmware from the BMC. The user can see the progress on the screen as shown in Figure 10.

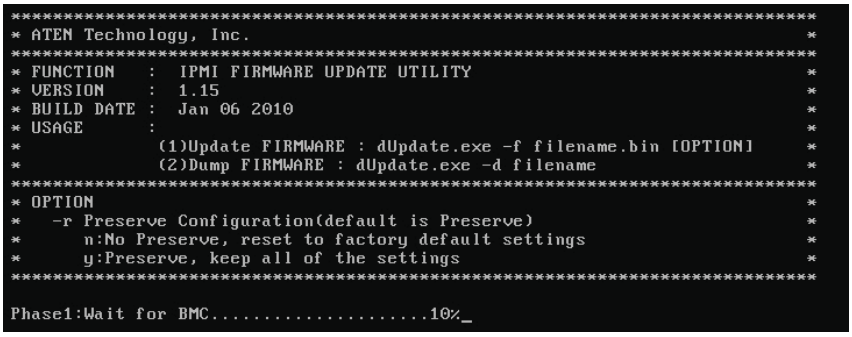

* ATEN Technology, Inc. *
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY *
* VERSION : 1.15 *
* BUILD DATE : Jan 06 2010 *
* USAGE : *
* (1)Update FIRMWARE : dUpdate.exe -f filename.bin [OPTION] *
* (2)Dump FIRMWARE : dUpdate.exe -d filename *
* OPTION *
* -r Preserve Configuration(default is Preserve) *
* n:No Preserve, reset to factory default settings *
* y:Preserve, keep all of the settings *
Phase1:Wait for BMC.....10%_

Figure 9: Phase 1- Flash Tools Waiting for the BMC to Prepare Data

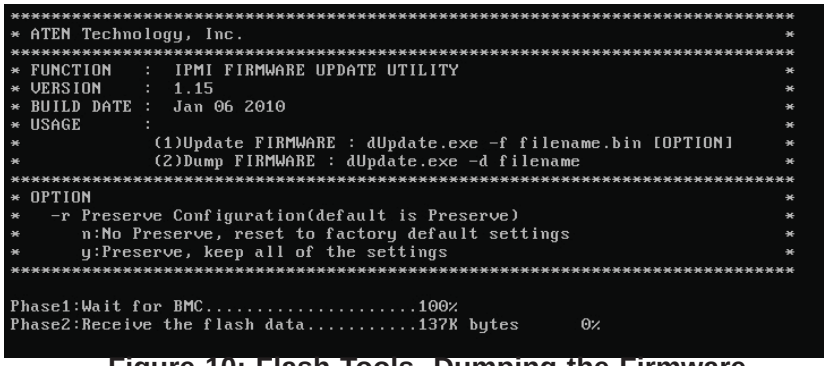

* ATEN Technology, Inc.
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY
* VERSION : 1.15
* BUILD DATE : Jan 06 2010
* USAGE :
(1)Update FIRMWARE : dUpdate.exe -f filename.bin [OPTION]
(2)Dump FIRMWARE : dUpdate.exe -d filename
* OPTION
-r Preserve Configuration(default is Preserve)
n:No Preserve, reset to factory default settings
y:Preserve, keep all of the settings
Phase1:Wait for BMC.....100%
Phase2:Receive the flash data.....137K bytes 0%

Figure 10: Flash Tools Dumping the Firmware

A-4 Windows/Linux Version of Flash Tools

In addition to DOS, Aten's Flash Tools Utility supports Windows and Linux platforms.

The Windows/Linux version of Flash Tools Utility provides the same features supported by the DOS version. In addition, it also allows the user to update the firmware via LAN connections.

The main screen of the Windows/Linux version displays the information about the firmware and the instructions on how to use the utility as shown in Figure 11.

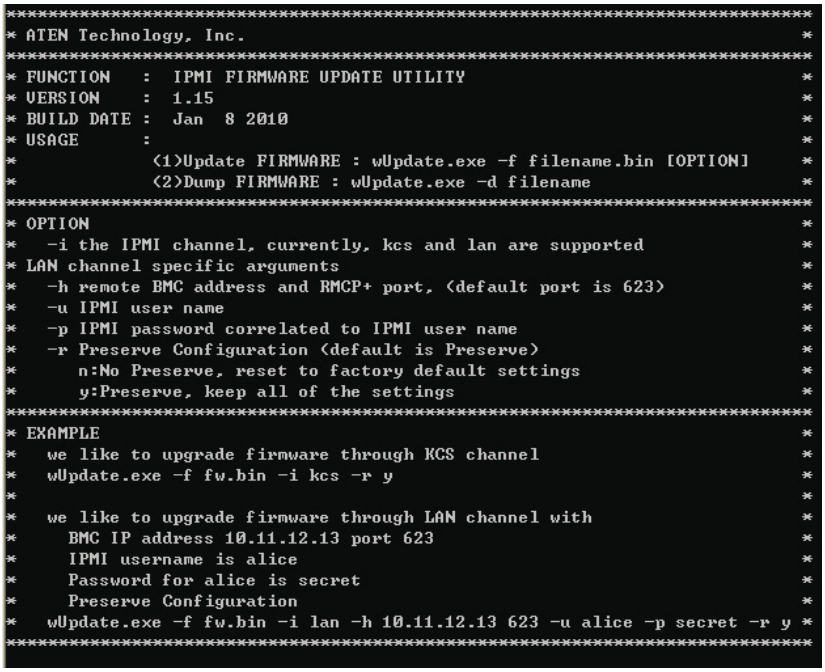

* ATEN Technology, Inc.
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY
* VERSION : 1.15
* BUILD DATE : Jan 8 2010
* USAGE :
(1)Update FIRMWARE : wUpdate.exe -f filename.bin [OPTION]
(2)Dump FIRMWARE : wUpdate.exe -d filename
* OPTION
-i the IPMI channel, currently, kcs and lan are supported
* LAN channel specific arguments
-h remote BMC address and RMCP+ port, (default port is 623)
-u IPMI user name
-p IPMI password correlated to IPMI user name
-r Preserve Configuration (default is Preserve)
n:No Preserve, reset to factory default settings
y:Preserve, keep all of the settings
* EXAMPLE
we like to upgrade firmware through KCS channel
wUpdate.exe -f fw.bin -i kcs -r y
we like to upgrade firmware through LAN channel with
BMC IP address 10.11.12.13 port 623
IPMI username is alice
Password for alice is secret
Preserve Configuration
wUpdate.exe -f fw.bin -i lan -h 10.11.12.13 623 -u alice -p secret -r y

Figure 11 Main Screen of Flash Tools (in the Windows/Linux Version)

In the Windows/Linux version of the Flash Tools Utility, there are six parameters:

(1) –f: Type <-f> to enter the filename of the firmware that you want to update.

(2) –i: *-i* indicates the IPMI channel. Currently, KCS and LAN connections are supported. If a LAN connection is used, the user needs to enter the following parameters:

1. –h: Type <-h> to enter the addresses of the remote BMC and the RMCP+ port (default port is 623).

2. –u: Type <-u> to enter the IPMI username.

3. –p: Type <-p> to enter the password for the IPMI user.

4. –r: Type <-r> to preserve (to save) the configuration settings you've entered. (This feature is optional.) (Default: preserve configuration.)

5. -y: Type <-y> for the BMC to keep all settings after updating the firmware; otherwise, the BMC will reset the settings to factory default.

To connect IPMI via KCS, type <wUpdate.exe/lUpdate –f [filename.bin] –I kcs –r y> as shown in Figure 12.

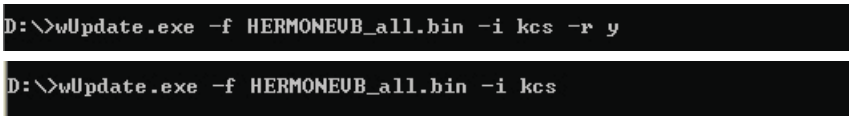


Figure 12: Example of KCS FW Updates with/without Preserving Configuration

To connect IPMI via LAN, type <wUpdate.exe/lUpdatewUpdate.exe -f [filename.bin] -i lan -h 192.168.46.65 623 -u alice -p secret -r y> as shown in Figure 13.

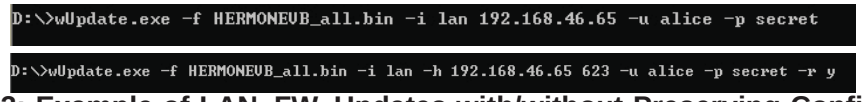

D:\>wUpdate.exe -f HERMONEVB_all.bin -i lan 192.168.46.65 -u alice -p secret
D:\>wUpdate.exe -f HERMONEVB_all.bin -i lan -h 192.168.46.65 623 -u alice -p secret -r y

Figure 13: Example of LAN_FW_Updates with/without Preserving Configuration and RMCP+ Port

For other settings, please refer to their counterparts in the DOS version for configuration instructions.

Notes

Appendix B

Introduction to SMASH

B-1 Overview

The SMASH (System Management Architecture for Server Hardware) platform, developed by Distributed Management Task Force, Inc. (DMTF), delivers a host of architecture-based, industry-standard protocols that will allow IT professionals to simplify the task of managing multiple network systems in a data center. SMASH offers a simple, intuitive solution to manage heterogeneous servers in a web environment regardless of their differences in hardware, software, OS, or network configuration. SMASH provides the end-user and the ISV community with interoperable management technology for multi-vendor server platforms.

How SMASH works

SMASH simplifies typical SMASH scripts by reducing commands to simple verbs. Although designed to manage multi-servers as a whole, SMASH can address individual components in a specific machine by using the SSH command-line protocol. Even when multiple processors, add-on cards, logical devices, and cooling systems are installed in a server, SMASH can be directed at a particular component in the server. A manager can use a text console to access, monitor, and manage all servers that are connected to the same SSL connection. SMASH can be programmed to periodically check all sensors in all machines or monitor a particular component in a specific server at any time. By adjusting the scope of tasks and the schedules of monitoring, SMASH allows the IT professionals to effectively manage multi-system clusters, minimize power consumption, and achieve system management efficiency.

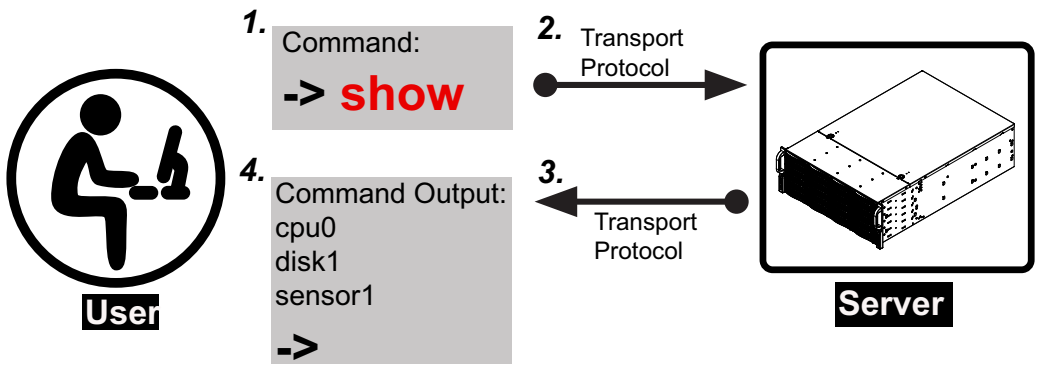


Figure B.1 SMASH-CLP User Interface

SMASH Compliance Information

SMASH documented in this user's guide is developed in reference to and in compliance with the SMASH Initiative Standards based on the following DMTF documents.

- System Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP) Architecture White Paper (DSP 2001)
- SM CLP Specification (DSP 0214)
- SM ME Addressing Specifications (DSP 0215)
- SM SLP to CIM Common Mapping Specification (DSP 0216)
- Common Information Model (CIM) Infrastructure Specification (DSP0004)
- The Secure Shell (SSH) Protocol Architecture (RFC4251)
- The Secure Shell (SSH) Connection Protocol (RFC4254)

B-2 An Important Note to the User

The information included in this user's guide provides a general guideline on how to use the SMASH protocol for your system management. Instructions given in this document may or may not be applicable to your system; it depends on the configuration of the system or the environment it operates in.

B-3 Using SMASH

This section provides a general guideline on how to use SMASH for your system management in a web-based environment. Refer to the SMASH script provided below to curtail a server management protocol for your systems.

Note: The instructions listed below are applicable to both Windows and Linux systems. We use the Windows platform as our default setting.

B-4 Initiating the SMASH Protocol

There are two ways of initiating the SMASH protocol.

To Initiate SMASH Automatically

You can initiate SMASH automatically by connecting the BMC (Baseboard Management Controller) via the Secure Shell protocol (SSH) from a client machine.

To connect from a Linux machine

1. Use 'ssh<BMC ip address>'.
2. Enter the password.

To connect from other machines

1. Use a terminal emulator application such as *Putty*.
2. Enter the *BMC ip* address in the terminal emulator application.
3. Choose *ssh* as the connection type
4. Enter the password at the prompt.
5. At the prompt '#", enter <SMASH> to invoke the SMASH prompt '—>'.
6. If you have successfully logged in, the SMASH prompt will display.

B-5 SMASH-CLP Main Screen

After you've successfully logged in the SSL network, the SMASH Command Line Protocol Main screen will display as shown below.

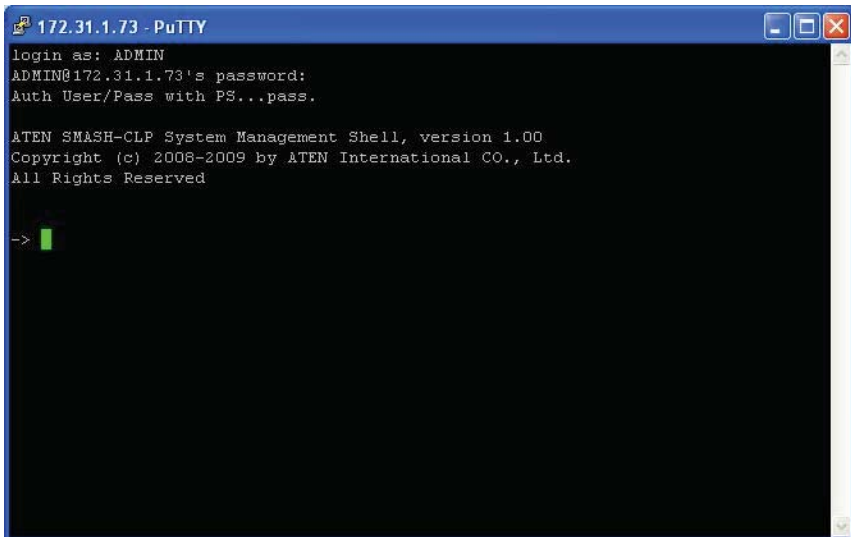


Figure B-2 SMASH-CLP Main Screen

B-6 Using SMASH for System Management

After you've familiarized yourself with SMASH commands, you are able to use these commands to manage your system. To properly manage your network system, be sure to follow the instructions below.

Note:

Make sure that the format of all your commands are compliant with the DMTF specification, which is "<Verb> [<option>] [<target>] [<properties>]", where:

- A ***Verb*** means a *command*.
- An ***Option*** works according to the definition of a command given in Section 7: Definitions of Command Verbs.
- A ***Target*** is a managed device which is also referred to in the diagram of *Target Addressing* as shown in Figure 2.1.
- ***Properties*** are the specific attributes that you want to assign to a target machine or to get from a target machine.

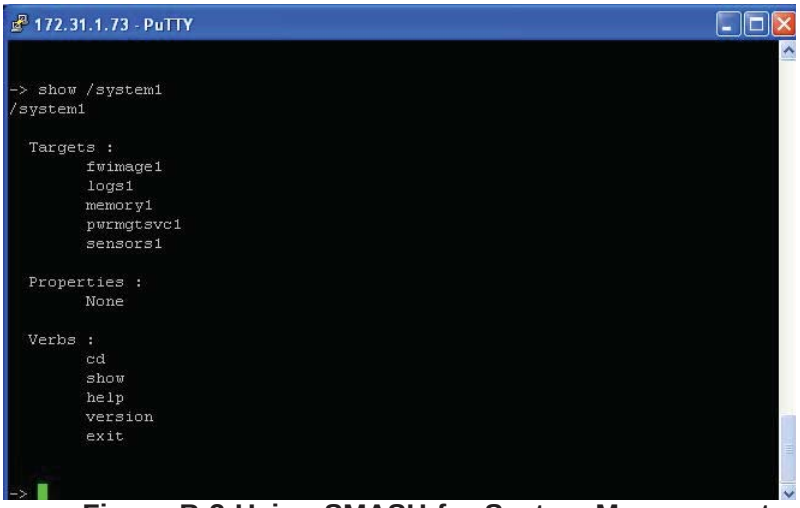


Figure B-3 Using SMASH for System Management

B-7 Definitions of Command Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow the user to issue commands to a target system to perform certain tasks. For example, the verbs supported by the *admin* target group include: cd, help, load, dump, create, delete, exit, version and show etc.

- ***cd***

The command verb *cd* is used to navigate to a specific target address using the SSL protocol. For example, issuing the command *cd/admin1* will direct you to the target *admin* (AdminDomain).

- ***show***

The command verb *show* is used to display the properties and the contents of a target, a group of targets, a sub-groups of the target(s). Properties, contents, supported operations related to the target, the group of targets or their sub-targets will be displayed.

- ***exit***

The command verb *exit* is used when you want to exit from a SMASH session or close a session.

- ***help***

The command verb *help* is used when you want to get helpful hints or information on a context-specific item. This command has the same function as the *help option* listed for the target group.

- ***Version***

Use the command verb *version* to display the CLP version used in a specific machine.

- ***set***

Use the command verb *set* to assign a set of values to the properties of a target machine.

- ***start***

The command verb *start* is used to turn on the power control, to start a process, or to change an operation state from a lower level to a higher level in a system.

- ***stop***

The command verb *stop* is used to turn off the power, to stop a process, or to change an operation state from a higher level to a lower level.

- ***reset***

The command verb *reset* is used to enable or to disable the power control of or the processes of the machine.

- ***delete***

The command verb *delete* is used to delete or to destroy an entry or a value previously entered. It can only be used in a specific target as defined according to the SAMSHCLP Standards.

- ***load***

The command verb *load* is used to move a binary image file from a URI source to the MAP. This command will achieve different results depending on the setting of a target system, and how the verb *load* is defined in the DSP specification used in the system.

- ***dump***

The command verb *dump* is used to move a binary image file from the MAP to a URI source. This command will achieve different results depending on the setting of a target system, and how the verb *dump* is defined in the DSP specification implemented in the system.

- ***create***

The command verb *create* is used to create a new address entry or a new item in the MAP. It can only be used in a specific target as defined in the SMASH profile or in MAP specifications.

B-8 SMASH Commands

The following table provides the definitions and the descriptions of SMASH commands. The most useful commands are *show* and *help*, which will provide the user with useful information on how to navigate through the SSL network connection.

Option Name	Short Form	Definition	Notes
-all	-a	Instructs a command verb to perform all tasks possible	None
-destination <*URI*>	None	Indicates the final location of an image or selected data	URI or SM instance address
-display	-d	Selects data that the user wishes to display	This can generate multiple query results
-examine	-x	Instructs the Command Processor to examine a command for syntax or semantic errors without executing it	None
-force	-f	Instructs the verb to ignore any warnings triggered by default but go ahead executing the command instead	None
-help	-h	Displays all information and documentation regarding the command verb	None
-keep <m[.s]	-k	Sets a time period to hold and keep the Job ID and the status of a command	The amount of time set to hold a command Job ID or its status can differ.
-level <n>	-l	Instructs the Command Processor to execute the command for the current target and for all target machines within the level specified by the user	Levels should be expressed in a nature number or "all".
-Output <args>	-o	Controls the format and the content of a command output. This only supports "format=clpxml" and "format=keyword"	Many variables or factors can affect the outcome of format, language, level of details of the output.
-Source <URI>	None	Indicates the location of a source image or a target	URI or SM Instance Address
-Version	-v	Displays the version of the command verb	None
-Wait	-w	Instructs the Command Processor to hold the command response or query result until all spawned jobs are completed.	None

Table B-1 SMASH Commands

B-9 Standard Command Options

The following table lists the standard command options.

CLP Option	CLP Verbs												
	CD	Create	delete	dump	exit	help	load	reset	set	show	start	Stop	version
all										x			
destination				x									
display										x			
examine	x	x	x	x	x	x	x	x	x	x	x	x	x
force			x	x			x	x	x	x	x	x	
help	x	x	x	x	x	x	x	x	x	x	x	x	x
keep													
level										x			
Output	x	x	x	x	x	x	x	x	x	x	x	x	x
Source							x						
Version	x	x	x	x	x	x	x	x	x	x	x	x	x
Wait													

Table B-2 Standard Command Options

B-10 Target Addressing

To simplified the process of SMASH command execution, a file system called Target Addressing was created as shown in the diagram below.

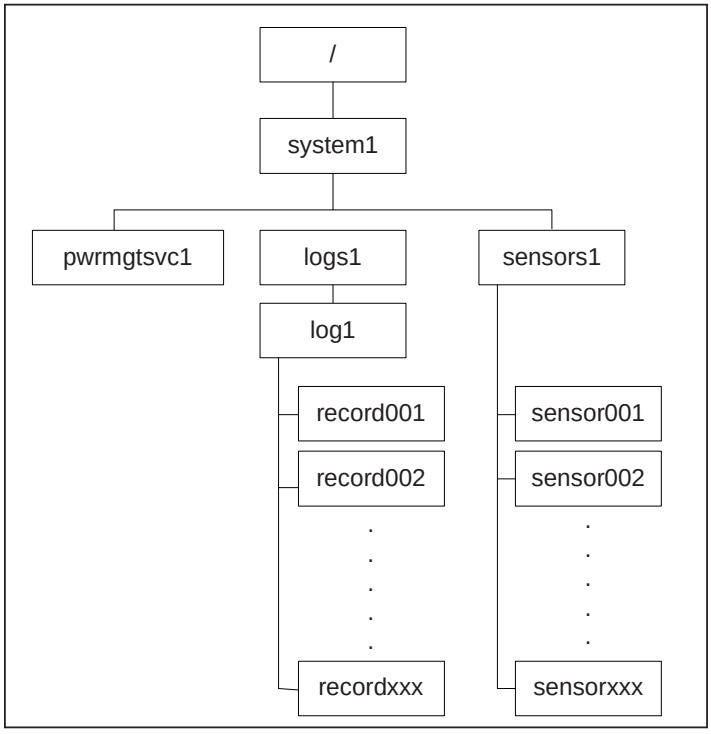


Figure B-4 Target Addressing Diagram

Terms Used in the Target Addressing Diagram

This section provides the descriptions of the terms used in the Target Addressing Diagram above.

- ***"/"*** indicates *the root* of the system.
- ***"/system1"*** includes all major *Targets*.
- ***"/system1/logs1/log1"*** includes all senor event logs.
- ***"/system1/sensors1"*** contains the readings and information of all sensors.
- ***"/system1/pwrmgtsvc1"*** is used for chassis control.
- ***"show../logs1"*** allows you to issue SMASH commands for the system to perform the tasks of your choice. For example:
  - Issuing the command ***"show/system1/logs1"*** *while you are in* ***"show../logs1"*** will allow you to set the *Absolute* or the *Relative* target path.

Notes

(Disclaimer Continued)

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.